Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 3

Carlos Gustavo Moreira e Samuel Barbosa Feitosa

Aula 1

Divisibilidade 1

Teorema 1. *(Algoritmo da Divisão) Para quaisquer inteiros positivos a e b, existe um único par (q, r) de inteiros não negativos tais que $b = aq + r$ e $r < a$. O número q e r são chamados de quociente e resto, respectivamente, da divisão de b por a.*

Definição 2. *Dados dois inteiros a e b, com $a \neq 0$, dizemos que a divide b ou que a é um divisor de b ou ainda que b é um múltiplo de a e escrevemos $a \mid b$ se o r dado pelo teorema anterior é 0, ou seja, se $b = aq$ para algum inteiro q.*

Lema 3. *Sejam a, b, c, d inteiros. Temos*

i) ("d divide") Se $d \mid a$ e $d \mid b$, então $d \mid ax + by$ para quaisquer x e y inteiros.

ii) ("Limitação") Se $d \mid a$, então $a = 0$ ou $|d| \leq |a|$.

iii) (Transitividade) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

Demonstração. Se $d \mid a$ e $d \mid b$, então podemos escrever $a = dq_1$ e $b = dq_2$ com $q_1, q_2 \in \mathbb{Z}$, logo $ax + by = d(q_1x + q_2y)$. Como $q_1x + q_2y \in \mathbb{Z}$, temos $d \mid ax + by$. Para mostrar *(ii)*, suponha que $d \mid a$ e $a \neq 0$. Neste caso, $a = dq$ com $q \neq 0$, assim $|q| \geq 1$ e $|a| = |d||q| \geq |d|$. Finalmente, se $a \mid b$ e $b \mid c$, então existem $q_1, q_2 \in \mathbb{Z}$ tais que $b = aq_1$ e $c = bq_2$, logo $c = aq_1q_2$ e portanto $a \mid c$. □

Em particular, segue da propriedade i) que $d \mid a + b$ e $d \mid a - b$.

Exemplo 4. *(Olimpíada de Maio 2006) Encontre todos os naturais a e b tais que $a|b+1$ e $b|a+1$.*

Pela propriedade da Limitação, temos $a \leq b + 1$ e $b \leq a + 1$. Daí, $a - 1 \leq b \leq b + 1$. Vejamos os casos:

(i) $a = b$. Como $a|b + 1$ e $a \mid b$(pois $b = a$) temos que $a \mid [(b + 1) - b] = 1$. Assim $a = 1$ Neste caso, só temos a solução $(a, b) = (1, 1)$

(ii) $a = b + 1$. Como $b|a + 1$ e $b|a - 1$(pois $b = a - 1$) temos que $b|[(a + 1) - (a - 1)] = 2$. Assim $b = 1$ ou $b = 2$ neste caso, só temos as soluções $(3, 2)$ e $(2, 1)$.

(iii) $a = b - 1$. Este caso é análogo ao anterior e as soluções para (a, b) são $(1, 2)$ e $(2, 3)$.

Exemplo 5. *Observe que, para quaisquer x e y vale:*

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \ldots + x^2y^{n-3} + xy^{n-2} + y^{n-1}).$$

Se n é ímpar, vale:

$$x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + x^{n-3}y^2 - \ldots + x^2y^{n-3} - xy^{n-2} + y^{n-1})$$

e se $n = 2k$ é par vale:

$$x^n - y^n = x^{2k} - y^{2k} = (x^2 - y^2)(x^{2k-2} + x^{2k-4}y^2 + x^{2k-6}y^4 + \ldots + x^4y^{2k-6} + x^2y^{2k-4} + y^{2k-2}) =$$

$$= (x + y)(x - y)(x^{2k-2} + x^{2k-4}y^2 + x^{2k-6}y^4 + \ldots + x^4y^{2k-6} + x^2y^{2k-4} + y^{2k-2}).$$

Assim, em particular, $10^n - 1$ é múltiplo de 9 para todo natural n, $10^n + 1$ é múltiplo de 11 para todo n ímpar e $10^n - 1$ é múltiplo de 11 para todo n par. Daí segue que, se a representação decimal de n é $a_k a_{k-1} ... a_1 a_0$ (i.e., se $n = a_0 + 10a_1 + ... + 10^k.a_k$), então n deixa o mesmo resto na divisão por 9 que $a_0 + a_1 + ... + a_k$, e n deixa o mesmo resto na divisão por 11 que $a_0 - a_1 + ... + (-1)^k.a_k$.

Exemplo 6. *(Critério de Divisibilidade por 7) Existem alguns métodos práticos para decidirmos se um número é múltiplo de outro. Certamente o leitor já deve ter se deparado com algum critério de divisibilidade. Existe um critério por 7 bastante popular: Para saber se um inteiro é múltiplo de 7, basta apagar seu último dígito, multiplicá-lo por 2 e subtrair do número que restou. Se o resultado é múltiplo de 7, então o número original também é múltiplo de 7.*

Podemos aplicar esse algoritmo sucessivas vezes até que o resultado obtido seja facilmente verificável como um múltiplo de 7. Por exemplo, para o número 561421 podemos escrever:

$$\begin{aligned} 56142 - 2 &= 56140 \\ 5614 - 0 &= 5614 \\ 561 - 8 &= 553 \\ 55 - 6 &= 49 \end{aligned}$$

Como 49 é múltiplo de 7, nosso número original também é. Por que esse processo funciona? Se o nosso número original está escrito na forma $10a + b$ então o número obtido após a operação descrita é $a - 2b$. Basta mostrarmos que se $7 \mid a - 2b$ então $7 \mid 10a + b$. Se $7 \mid a - 2b$, pela propriedade (i) do lema, concluímos que $7 \mid 10a - 20b$. Como $7 \mid 21b$, também temos que $7 \mid [(10a - 20b) + 21b] = 10a + b$.

Exemplo 7. *Mostre que se $7 \mid 3a + 2b$ então $7 \mid 4a - 2b$.*

Veja que $7 \mid 7a$ e $7 \mid 3a+2b$, então $7 \mid [7a-(3a+2b)] = 4a-2b$. Na prática, o que fizemos foi multiplicar o número $3a+2b$ por algum inteiro e logo em seguida subtraímos um múltiplo de 7 conveniente para obter o número $4a-2b$. Existem outras formas de fazermos isso. Observe os números $3\cdot 0, 3\cdot 1, 3\cdot 2, 3\cdot 3, 3\cdot 4, 3\cdot 5, 3\cdot 6$. O número $3\cdot 6$ deixa o mesmo resto que 4 por 7, pois $3\cdot 6 = 7\cdot 2+4$. Como $7|3a+2b$ podemos concluir que $7|(18a+12b)$ e consequentemente $7 \mid [18a+12b-14a)] = 4a+12b$. Mas $7 \mid 14b$, então $7 \mid [4a+12b-14b] = 4a-2b$.

Exemplo 8. *(Olimpíada de Leningrado 1989) Seja A um número natural maior que 1, e seja B um número natural que é um divisor de A^2+1. Prove que se $B-A>0$, então $B-A>\sqrt{A}$.*

Seja $B-A=q$. Assim, $A+q \mid A^2+1$. Como $(A-q)(A+q) = A^2-q^2$ é divisível por $A+q$, podemos concluir que $A+q \mid [(A^2+1)-(A^2-q^2)] = q^2+1$. Pela propriedade de limitação, $A+q \leq q^2+1$. Nessa desigualdade, não podemos ter $q=1$ pois $A>1$. Usando então que $q>1$, temos $A \leq q^2-q+1 < q^2$, ou seja, $\sqrt{A} < q$.

Exemplo 9. *Encontre todos os inteiros positivos n tais que $2n^2+1 \mid n^3+9n-17$.*

Utilizando o "$2n^2+1$ divide" para reduzir o grau de $n^3+9n-17$, temos que

$$\begin{aligned} &\begin{cases} 2n^2+1 \mid n^3+9n-17 \\ 2n^2+1 \mid 2n^2+1 \end{cases} \\ \implies & 2n^2+1 \mid (n^3+9n-17)\cdot 2 + (2n^2+1)\cdot(-n) \\ \iff & 2n^2+1 \mid 17n-34 \end{aligned}$$

Como o grau de $17n-34$ é menor do que o de $2n^2+1$, podemos utilizar a "limitação" para obter uma lista finita de candidatos a n. Temos $17n-34=0 \iff n=2$ ou $|2n^2+1| \leq |17n-34| \iff n = 1, 4$ ou 5. Destes candidatos, apenas $n=2$ e $n=5$ são soluções.

Exemplo 10. *(Leningrado 1990) Sejam a e b números naturais tais que b^2+ba+1 divide a^2+ab+1. Prove que $a=b$.*

Pela propriedade de limitação, $b^2+ba+1 \leq a^2+ab+1$ e daí $b \leq a$. Além disso, $b^2+ab+1 > a-b$. A igualdade $b(a^2+ab+1)-a(b^2+ba+1) = b-a$ implica que $a-b$ é divisível por b^2+ba+1. Se $a-b \neq 0$, então $b^2+ab+1 \leq a-b$. Mas isso é um absurdo, logo $a-b=0$.

Exemplo 11. *(IMO 1998) Determine todos os pares de inteiros positivos (x,y) tais que xy^2+y+7 divide x^2y+x+y.*

A igualdade $y(x^2y+x+y)-x(xy^2+y+7) = y^2-7x$ implica que y^2-7x é divisível por xy^2+y+7. Se $y^2-7x \geq 0$, então como $y^2-7x < xy^2+y+7$, segue que $y^2-7x=0$. Então $(x,y) = (7t^2, 7t)$ para algum $t \in \mathbb{N}$. É fácil checar que esses pares são realmente soluções. Se $y^2-7x<0$, então $7x-y^2>0$ é divisível por xy^2+y+7. Mas daí, $xy^2+y+7 \leq 7x-y^2 < 7x$, que implica $y \leq 2$. Para $y=1$, temos $x+8 \mid 7x-1 \Rightarrow x+8 \mid 7(x+8)-(7x-1) = 57$. Então

as únicas possibilidades são $x = 11$ e $x = 49$ e os pares correspondentes são $(11, 1), (49, 1)$ que obviamente são soluções. Para $y = 2$ temos $4x + 9 \mid 7x - 4$ e consequentemente $7(4x+9) - 4(7x-4) = 79$ é divisível por $4x+9$. Nesse caso não obtemos nenhuma solução nova. Todas as soluções (x, y): $(7t^2, 7t)(t \in \mathbb{N}), (11, 1)$ e $(49, 1)$.

Problemas Propostos

Problema 12. *i) Mostre que* $3 \mid a + 7b$ *então* $3 \mid a + b$.

ii) Mostre que $7 \mid a + 3b$ *então* $\mid 13a + 11b$

iii) Mostre que $19 \mid 3x + 7y$ *então* $19 \mid 43x + 75y$

iv) Mostre que $17 \mid 3a + 2b$ *então* $17 \mid 10a + b$

Problema 13 (IMO1959)**.** *Mostre que a fração* $\frac{21n+4}{14n+3}$ *é irredutível para todo* n *natural.*

Problema 14. *Encontre todos os inteiros positivos tais que*

(a) $n + 1 \mid n^3 - 1$

(b) $2n - 1 \mid n^3 + 1$

(c) $\frac{1}{n} + \frac{1}{m} = \frac{1}{143}$

(d) $2n^3 + 5 \mid n^4 + n + 1$

Problema 15. *Prove que se* $f(x)$ *é um polinômio com coeficientes inteiros e* a *e* b *são inteiros quaisquer, então* $a - b \mid f(a) - f(b)$.

Problema 16. *(Bielorússia 1996) Inteiros* m *e* n*, satisfazem a igualdade*

$$(m - n)^2 = \frac{4mn}{m + n - 1}$$

a) Prove que $m + n$ *é um quadrado perfeito*

b) Encontre todos os pares (m, n) *satisfazendo a equação acima.*

Problema 17. *Seja* $n > 1$ *e* k *um inteiro positivo qualquer. Prove que* $(n-1)^2 | (n^k - 1)$ *se, e somente se ,* $(n - 1) | k$.

Problema 18. *(OBM 2005) Prove que a soma* $1^k + 2^k + \ldots n^k$*, onde* n *é um inteiro e* k *é ímpar, é divisível por* $1 + 2 + \ldots + n$.

Problema 19. *(OBM 2000) É possível encontrar duas potências de 2, distintas e com o mesmo número de algarismos, tais que uma possa ser obtida através de uma reordenação dos dígitos da outra? (Dica: Lembre-se do critério de divisibilidade por 9)*

Problema 20. *Encontre todos os inteiros positivos n tais que $n+2009$ divide n^2+2009 e $n+2010$ divide n^2+2010.*

Problema 21. *(IMO 2003)Encontre todos os pares de inteiros positivos (m,n) tais que*

$$\frac{m^2}{2mn^2-n^3+1}$$

é um inteiro positivo.

Problema 22. *(IMO 1994) Encontre todos os pares ordenados (m,n) onde m e n são inteiros positivos tais que $\frac{n^3+1}{mn-1}$ é um inteiro.*

Problema 23. *Prove que para qualquer inteiro positivo m, existe um número infinito de pares de inteiros (x,y) satisfazendo as condições:*

1. *x e y são primos entre si;*
2. *y divide x^2+m;*
3. *x divide y^2+m.*

Dicas e Soluções

12. Como $3 \mid 6b$, segue que $3 \mid [(a+7b)-6b] = a+b$.

    Como $7 \mid a+3b$, segue que $7 \mid 13a+39b = (13a+11b)+28b$. Mas $7 \mid 28b$, portanto $7 \mid [(13a+11b)+28b-28b] = 13a+11b$.

    Como $19 \mid 3x+7y$, segue que $19 \mid 27(3x+7y) = (43x+75y)+(38x+114y)$. Mas $19 \mid 19(2x+6y)$, portanto $19 \mid [(43x+75y)+(38x+114y)-19(2x+6y)] = 43x+75y$.

    Como $17 \mid 3a+2b$, segue que $17 \mid 27a+18b = (10a+b)+17(a+b)$.

16. Somando $4mn$ em ambos os lados, obtemos:

$$\begin{aligned}(m+n)^2 &= \frac{4mn}{m+n-1}+4mn \\ &= \frac{4mn(m+n)}{m+n-1} \Rightarrow \\ (m+n) &= \frac{4mn}{m+n-1} \\ &= (m-n)^2.\end{aligned}$$

    Assim, $m+n$ é o quadrado de um inteiro. Se $m-n=t$, então $m+n=t^2$ e $(m,n) = (\frac{t^2+t}{2}, \frac{t^2-t}{2})$. É fácil verificar que para qualquer t inteiro esse par é solução do problema.

17. Veja que

$$\frac{n^k-1}{(n-1)^2} = \left(\frac{n^{k-1}-1}{n-1} + \frac{n^{k-2}-1}{n-1} + \ldots + \frac{n-1}{n-1} + \frac{k}{n-1}\right).$$

Como os números $\frac{n^l-1}{n-1}$ sempre são inteiros, o número do lado esquerdo da equação será inteiro se, e somente se, o número $\frac{k}{n-1}$ for inteiro.

18. Comece dividindo o problema quando em dois casos: n é par ou n é ímpar. Sabemos que $1+2+\ldots+n = \frac{n(n+1)}{2}$. Para n ímpar, basta mostrar que o número em questão é divisível por n e $\frac{n+1}{2}$. O próximo passo é lembrar do problema 33 da aula 1. Pela fatoração de $x^n + y^n$, temos que $i^k + (n-i)^k$ é divisível por n. Faça outros tipos de pares para mostrar a divisibilidade por $\frac{n}{2}$. O caso quando n é par é análogo.

20. Analise a expansão pelo binômio de Newton.

21. Não. Suponha, por absurdo, que existam duas potências de 2, $2^m < 2^n$, satisfazendo o enunciado. Como 2^n é um múltiplo de 2^m, podemos ter: $2^n = 2\cdot 2^m, 4\cdot 2^m, 8\cdot 2^m, \ldots$. Além disso, como ambos possuem a mesma quantidade de dígitos, temos $1 < \frac{2^n}{2^m} < 10$. Assim, as únicas possibilidade são $2^n = 2\cdot 2^m, 4\cdot 2^m, 8\cdot 2^m$. Pelo critério de divisibilidade por 9, como 2^m e 2^n possuem os mesmos dígitos, podemos concluir que $2^n - 2^m$ é um múltiplo de 9. Entretanto, nenhuma das possibilidade anteriores satisfaz essa condição e chegamos em um absurdo.

Referências

[1] F. E. Brochero Martinez, C. G. Moreira, N. C. Saldanha, E. Tengan - Teoria dos Números - um passeio com primos e outros números familiares pelo mundo inteiro, Projeto Euclides, IMPA, 2010.

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

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

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

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

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