Teoria dos Números

notas de aula (PTOM/POTI)

Teoria dos Números

notas de aula (PTOM/POTI)

Ricardo Machado
Universidade Federal Rural de Pernambuco

February 22, 2023

Sobre Ricardo Machado Professor Adjunto da Universidade Federal Rural de Pernambuco, DM.

Doutor em Matemática pela Universidade Federal de Pernambuco (2009-2013).

Mestre em Matemática pela Universidade Federal de Pernambuco (2007-2009).

Bacharel em Matemática pela Universidade Federal de Pernambuco (2003-2006).

Prefácio

Ricardo Machado
Recife, 2023

Sumário

Capítulo 1

Divisibilidade

Realização:

Apoio:

1.1 Aula 01 - Divisibilidade I

Teorema 1.1.1 (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 $r < a$. Os números q e r são chamados de quociente e resto, respectivamente, da divisão de b por a.*

Exemplo 1.1.2

$$5 = 3 \cdot 1 + 2, \quad r = 2 < 3 = a;$$

$$7 = 9 \cdot 7 + 0, \quad r = 7 < 9 = a;$$

□

Tecnologia 1.1.3 Abaixo temos um código em SageMath, no qual podemos trocar os valores de b e a nas linhas 1 e 2, respectivamente. Ao clicar em Executar (Sage) obtemos o quociente e o resto na divisão de b por a.

```
b=13
a=5
(q,r) = (b//a, b%a)
print('%d = %d*%d + %d' %(b,a,q,r))
```

Observação 1.1.4 O teorema anterior admite um enunciado mais geral: Para quaisquer inteiros a e b, com $a \neq 0$, existe um único par de inteiros (q, r) tais que $b = aq + r,\ 0 \leq r < |a|$. Por exemplo,

$$-7 = -3 \cdot 3 + 2, \quad r = 2 < |-3| = a.$$

Observação 1.1.5 (PTOM). De modo geral, fixado um número natural $a \geq 2$, pode-se sempre escrever um número qualquer b, de modo único, na forma $b = aq + r$, na qual q, r são inteiros e $0 \leq r < a$.

Por exemplo, fixado um valor para a, qualquer inteiro b pode ser escrito em

apenas uma das seguintes formas

$$\begin{aligned} &a = 3 : 3q, 3q+1, 3q+2 \\ &a = 4 : 4q, 4q+1, 4q+2, 4q+3 \\ &a = 5 : 5q, 5q+1, 5q+2, 5q+3, 5q+4 \\ &\quad\vdots \end{aligned}$$

Exemplo 1.1.6 (PTOM). Dados dois números primos $p < q$, dizemos que ele são *primos gêmeos* se $q-p = 2$. Prove que para cada par de primos gêmeos com $p < q$, se $p > 3$, então $p+1$ deixa resto zero na divisão por 3.**Solução**. Pela Observação **??**, p só pode assumir uma das três formas: $3k, 3k+1, 3k+2$. Podemos analizar cada um dos casos.

Caso 1 ($p = 3k$). Neste caso o número não seria primo, então este caso está descartado.

Caso 2 ($p = 3k+1$). Neste caso, $p+1 = 3k+2$ e $q = p+2 = 3k+3 = 3(k+1)$ não seria primo, o que é uma contradição.

Caso 3 ($p = 3k+2$). Neste caso, $p+1 = 3(k+1)$ que é múltiplo de 3 e $q = 3(k+1)+1$. Portanto, este é o único caso possível e o número $p+1$ sempre deixa resto zero na divisão por 3. □

Exemplo 1.1.7 Encontre um número natural N que, ao ser dividido por 10, deixa resto 9, ao ser dividido por 9 deixa resto 8, e ao ser dividido por 8 deixa resto 7.**Solução**. Pelos dados do enunciado,

$$\begin{aligned} N &= 10q_1 + 9 \\ N &= 9q_2 + 8 \\ N &= 8q_3 + 7 \end{aligned}$$

Somando 1 em cada igualdade, obtemos

$$\begin{aligned} N+1 &= 10q_1 + 10 = 10(q_1+1) \\ N+1 &= 9q_2 + 9 = 9(q_2+1) \\ N+1 &= 8q_3 + 8 = 8(q_3+1) \end{aligned}$$

Portanto, $N+1$ é múltiplo de 10, 9 e 8. Uma solução é $N+1 = 10 \cdot 9 \cdot 8 = 720$, logo $N = 719$.

Outra resposta pode ser obtida calculando o menor múltiplo comum: $MMC(10, 9, 8) = 360$. Outro valor válido para N é 359. □

Exemplo 1.1.8

a Verifique que

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1).$$

b Calcule o resto da Divisão de 4^{2012} por 3.

Solução. **item a)**

$$\begin{aligned} (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1) = a^n + a^{n-1} + a^{n-2} + \cdots + a^2 + a \\ - a^{n-1} - a^{n-2} - \cdots - a - 1 \end{aligned}$$

item b)

$$4^{2012} - 1 = (4-1)(4^{2011} + 4^{2010} + \cdots + 4 + 1)$$

$$= 3 \cdot \underbrace{(4^{2011} + 4^{2010} + \cdots + 4 + 1)}_{q}$$

Portanto,

$$4^{2012} = 3q + 1$$

Ou seja, o resto é igual a 1. □

Tecnologia 1.1.9 No SageMath, o resto da divisão de b^c por a pode ser calculado da seguinte maneira:

```
b=4
c=2012
a=3
pow(b,c,a)
```

Exemplo 1.1.10 Seja n um número natural maior que zero. Qual o resto de 10^n na divisão por 9?**Solução**.

$$\begin{aligned} 10^n - 1 &= (10-1)(10^{n-1} + 10^{n-2} + \cdots + 10 + 1) \\ 10^n - 1 &= 9q \\ 10^n &= 9q + 1 \end{aligned}$$

□

Exemplo 1.1.11 Quantos números entre 1 e 253 (inclusive) são divisíveis por 5? Ou seja, quando deixam resto zero na divisão por 5?**Solução**. Aplicando a divisão euclidiana,

$$253 = 5 \cdot 50 + 3.$$

Isto significa que existem 50 números divisíveis por 5 entre 1 e 253, pois ao escrever todos os números neste intervalo, o último que deixa resto zero será no número $5 \cdot 50 = 250$. Observe,

$$1, 2, 3, 4, \underbrace{5}_{5\cdot 1}, 6, \ldots, \underbrace{10}_{5\cdot 2}, \ldots, \underbrace{15}_{5\cdot 3}, \ldots \underbrace{250}_{5\cdot 50}, 251, 252, 253$$

□

Teorema 1.1.12 (Teorema dos Restos). *Se b_1 e b_2 deixam restos r_1 e r_2 na divisão por a, respectivamente, então:*

i $b_1 + b_2$ deixa o mesmo resto que $r_1 + r_2$ na divisão por a

ii $b_1 b_2$ deixa o mesmo resto que $r_1 r_2$ na divisão por a.

Demonstração. Por hipótese

$$b_1 = aq_1 + r_1,\ 0 \leq r_1 < a \quad \text{e} \quad b_2 = aq_2 + r_2,\ 0 \leq r_2 < a.$$

item a)

$$b_1 + b_2 = aq_1 + r_1 + aq_2 + r_2$$

$$b_1 + b_2 = a(q_1 + q_2) + r_1 + r_2. \tag{1.1.1}$$

Aplicando a divisão euclidiana obtemos

$$r_1 + r_2 = aq_3 + r_3,\ 0 \leq r_3 < a. \tag{1.1.2}$$

Substituindo (**??**) em (**??**) obtemos

$$b_1 + b_2 = a(q_1 + q_2 + q_3) + r_3,\ 0 \leq r_3 < a.$$

item b)

$$b_1b_2 = (aq_1 + r_1)(aq_2 + r_2)$$
$$b_1b_2 = a^2q_1q_2 + aq_1r_2 + aq_2r_1 + r_1r_2$$
$$b_1b_2 = a(aq_1q_2 + q_1r_2 + q_2r_1) + r_1r_2. \tag{1.1.3}$$

Aplicando a divisão euclidiana, podemos escrever

$$r_1r_2 = aq_4 + r_4,\ 0 \leq r_4 < a. \tag{1.1.4}$$

Substituindo (**??**) em (**??**) obtemos

$$b_1b_2 = a(aq_1q_2 + q_1r_2 + q_2r_1 + q_4) + r_4,\ 0 \leq r_4 < a.$$

Como queríamos. ■

Exemplo 1.1.13 Qual o resto que o número $1002 \cdot 1003 \cdot 1004$ deixa quando dividido por 7?**Solução**. Aplicando a divisão euclidiana, obtemos

$$1002 = 7 \cdot 143 + 1$$
$$1003 = 7 \cdot 143 + 2$$
$$1004 = 7 \cdot 143 + 3$$

Aplicando o (Teorema dos Restos), o resto de $1002 \cdot 1003 \cdot 1004$ na divisão por 7 é o mesmo que o resto de $1 \cdot 2 \cdot 3$ na divisão por 7. Como $1 \cdot 2 \cdot 3 = 6$ Temos,

$$1002 \cdot 1003 \cdot 1004 = 7 \cdot q + 6.$$

□

Exemplo 1.1.14 Qual o resto que o número 4^{5000} deixa quando dividido por 3?**Solução**. Como o número 4 deixa resto 1 na divisão por 3, 4^{5000} deixa o mesmo resto que $\underbrace{1 \cdot 1 \cdot 1 \cdots 1}_{5000} = 1$ na divisão por 3. □

Exemplo 1.1.15 Qual o resto que o número 2^{2k+1} deixa quando dividido por 3?**Solução**. Note que

$$2^{2k+1} = 2^{2k} \cdot 2 = 4^k \cdot 2.$$

- 4 deixa resto 1 na divisão por 3, logo 4^k também deixa resto 1 na divisão por 3;
- 2 deixa resto 2 na divisão por 3.

Pelo (Teorema dos Restos), 2^{2k+1} deixa o mesmo resto que $4^k \cdot 2$ na divisão por 3, ou seja, o resto é o mesmo que o resto de $1 \cdot 2 = 2$ na divisão por 3. □

Exemplo 1.1.16 Qual o resto de $n^3 + 2n$ na divisão por 3?**Solução**. Dado um número n, ele pode ser escrito em apenas uma das três formas: $3q, 3q + 1$ ou $3q + 2$. Pelo (Teorema dos Restos), basta analisar os três possíveis restos na divisão de n por 3.

Caso 1: $r = 0$:

$$0^3 + 2 \cdot 0 = 0 = 3 \cdot 0 + 0$$

Caso 2: $r = 1$:

$$1^3 + 2 \cdot 1 = 3 = 3 \cdot 1 + 0$$

Caso 3: $r = 2$:

$$2^3 + 2 \cdot 12 = 3 \cdot 4 + 0$$

□

Exemplo 1.1.17 Prove que, para cada n natural,

$$(n+1)(n+2)\cdots(2n)$$

é divisível por 2^n.**Solução**. Observe que

$$\begin{aligned}(n+1)(n+2)\cdots(2n) &= (n+1)(n+2)\cdots(2n)\cdot\frac{1\cdot 2\cdot 3\cdots n}{1\cdot 2\cdot 3\cdots n}.\\ &= \frac{1\cdot 2\cdot 3\cdots(2n-1)\cdot(2n)}{1\cdot 2\cdot 3\cdots n}.\end{aligned}$$

Para cada número k escrito no denominador, existe o número $2k$ no numerador. Agrupando as frações $\frac{2k}{k}$ com $1 \leq k \leq n$, sobrará todos os números ímpares de 1 até $2n$. Ou seja,

$$\begin{aligned}(n+1)(n+2)\cdots(2n) &= \frac{2\cdot 1}{1}\cdot\frac{2\cdot 2}{2}\cdots\frac{2\cdot n}{n}\cdot 1\cdot 3\cdot 5\cdots(2n-1)\\ &= 2^n\cdot 1\cdot 3\cdot 5\cdots(2n-1).\end{aligned}$$

□

Exemplo 1.1.18 Encontre todos os pares de inteiros positivos a e b tais que $79 = ab+2a+3b$.**Solução**. Note que $ab+2a+3b$ quase pode ser escrito como um produto, pois no produto "sobra" uma constante:

$$(a+3)(b+2) = ab+2a+3b+6.$$

Como

$$79 = ab+2a+3b,$$

ao somar 6 em ambos os membros da igualdade anterior, obtemos

$$85 = (a+3)(b+2).$$

Como 85 é o produto de dois primos $(5\cdot 17)$, então

$$5\cdot 17 = (a+3)(b+2).$$

Temos apenas dois casos:

$$\begin{cases} a+3 = 5 \Rightarrow a = 2\\ b+2 = 17 \Rightarrow b = 15\end{cases}$$

e

$$\begin{cases} a+3 = 17 \Rightarrow a = 14\\ b+2 = 5 \Rightarrow b = 3\end{cases}$$

□

Exemplo 1.1.19 (OBMEP 2013). Lucas pensou em um número, dividiu-o por 285 e obteve resto 77. Se ele dividir o número em que pensou por 57, qual o resto que ele vai encontrar?**Solução**. Note que $285 = 5\cdot 57$ e que $77 = 57+20$, logo

$$\begin{aligned}n &= 285\cdot q + 77\\ &= 5\cdot 57\cdot q + 57 + 20\end{aligned}$$

$$= 57(5 \cdot q + 1) + 20.$$

Portanto, o resto na divisão por 57 é 20. □

Exemplo 1.1.20 Encontre os inteiros que, na divisão por 7 deixam um quociente igual ao resto.**Solução**. Estamos procurando os números que podem ser escritos da seguinte maneira

$$n = 7q + r, (0 \leq r < 7) \quad \text{com } q = r. \tag{1.1.5}$$

São apenas 7 restos possíveis, podemos substituir esses valores em (**??**) para obter os valores de n.

$$\begin{aligned}
n = 7 \cdot 0 + 0 &\Rightarrow n = (7 + 1) \cdot 0 \Rightarrow n = 0 \\
n = 7 \cdot 1 + 1 &\Rightarrow n = (7 + 1) \cdot 1 \Rightarrow n = 8 \\
n = 7 \cdot 2 + 2 &\Rightarrow n = (7 + 1) \cdot 2 \Rightarrow n = 16 \\
n = 7 \cdot 3 + 3 &\Rightarrow n = (7 + 1) \cdot 3 \Rightarrow n = 24 \\
n = 7 \cdot 4 + 4 &\Rightarrow n = (7 + 1) \cdot 4 \Rightarrow n = 32 \\
n = 7 \cdot 5 + 5 &\Rightarrow n = (7 + 1) \cdot 5 \Rightarrow n = 40 \\
n = 7 \cdot 6 + 6 &\Rightarrow n = (7 + 1) \cdot 6 \Rightarrow n = 48
\end{aligned}$$

□

Exemplo 1.1.21 Ao dividir o número inteiro $20 + x$ por 11 obtemos resto 7. Qual é o menor valor inteiro positivo de x?**Solução**.

$$\begin{aligned}
20 + x &= 11q + 7 \\
x &= 11q - 13.
\end{aligned}$$

Como x é positivo, $q \geq 2$. Substituindo $q = 2$, obtemos

$$\begin{aligned}
x &= 11 \cdot 2 - 13 \\
&= 22 - 13 \\
&= 9.
\end{aligned}$$

□

Exemplo 1.1.22 (OBM). O número de seis dígitos $ab2016$ é um múltiplo de 99. Determine o valor do dígito a.**Solução**. Note que $100 = 99 \cdot 1 + 1$. Podemos escrever o número $ab2016$ da seguinte maneira:

$$\begin{aligned}
ab2016 &= ab \cdot 100^2 + 20 \cdot 100^1 + 16 \cdot 100^0 \\
&= ab(99q_2 + 1) + 20(99 \cdot 1 + 1) + 16(99 \cdot 0 + 1) \\
&= 99(ab \cdot q_2 + 20 \cdot 1 + 16 \cdot 0) + (ab + 20 + 16).
\end{aligned}$$

Portanto, 99 divide $ab2016$ se, e somente se, 99 divide $(ab + 20 + 16)$. Ou seja, como 99 possui dois diígitos e $(ab+20+16)$ é menor que $2 \cdot 99$, temos a seguinte igualdade

$$\begin{aligned}
99 &= ab + 36 \\
99 - 36 &= ab \\
63 &= ab.
\end{aligned}$$

Então, $a = 6$. □

1.1.1 Exercícios

1. Determinar os números que divididos por 17 dão um resto igual ao quadrado do quociente correspondente.

2. **(OCM 1985).** Encontre o quociente da divisão de $a^{128} - b^{128}$ por

$$(a^{64} + b^{64})(a^{32} + b^{32})(a^{16} + b^{16})(a^8 + b^8)(a^4 + b^4)(a^2 + b^2)(a + b).$$

3. **(OCM 1994).** Seja $A = 777\ldots777$ um número onde o dígito "7" aparece 1001 vezes. Determine o quociente e o resto da divisão de A por 1001.**Solução**. Observe que $A = 7\frac{10^{1001}-1}{9}$, e que $1001 = 10^3 + 1$. Como

$$\begin{aligned}(10^{999} + 1) &= ((10^3)^{333} + 1)\\ &= (10^3 + 1)((10^3)^{332} - (10^3)^{331} + (10^3)^{330} - \cdots + 1),\end{aligned}$$

Sabemos que $\frac{10^{999}+1}{10^3+1}$ é um número inteiro. Assim,

$$\begin{aligned}\frac{10^{1001} - 1}{10^3 + 1} &= 100 \cdot \frac{10^{999} + 1}{10^3 + 1} - \frac{101}{10^3 + 1}\\ &= 100 \cdot \frac{10^{999} + 1}{10^3 + 1} - \frac{1001 - 900}{10^3 + 1}\\ &= 100 \cdot \frac{10^{999} + 1}{10^3 + 1} - 1 + \frac{900}{10^3 + 1}\\ &= \frac{10^{1001} - 901}{10^3 + 1} + \frac{900}{10^3 + 1}.\end{aligned}$$

Dividindo ambos os membros da igualdade por 9 e em seguida multiplicando por 7, obtemos

$$\begin{aligned}\frac{10^{1001} - 1}{9(10^3 + 1)} &= \frac{10^{1001} - 901}{9(10^3 + 1)} + \frac{100}{10^3 + 1}\\ \frac{7 \cdot (10^{1001} - 1)}{9(10^3 + 1)} &= \frac{7 \cdot (10^{1001} - 901)}{9(10^3 + 1)} + \frac{700}{10^3 + 1}.\end{aligned}$$

Afirmação: $\frac{7\cdot(10^{1001}-901)}{9(10^3+1)}$ é inteiro e portanto

$$A = 1001 \cdot \frac{7 \cdot (10^{1001} - 901)}{9(10^3 + 1)} + 700.$$

Para concluir, vamos provar a afirmação acima. Observe que $1001 = 7 \cdot 11 \cdot 13$. Então, como $7, 9, 11, 13$ não possuem fatores primos em comum, para mostrar que $9(10^3 + 1)$ divide $7 \cdot (10^{1001} - 901)$, basta mostrar que cada um dos números $9, 11$ e 13 divide $(10^{1001} - 901)$.

i (9 divide $(10^{1001} - 901)$). Note que 10 deixa resto 1 na divisão por 9 e que -901 deixa resto 8, na divisão por 9. Assim, Pelo Teorema dos Restos, $(10^{1001} - 901)$ deixa o mesmo resto que $(1^{1001} + 8) = 9$ na divisão por 9, ou seja, o resto é zero.

ii (11 divide $(10^{1001} - 901)$). Como 10^2 deixa resto 1 na divisão por 11 e -901 deixa resto 1 na divisão por 11. Pelo Teorema dos restos, $(10^{1001} - 901)$ deixa o mesmo resto que $((1)^{500} \cdot 10 + 1) = 11$, na divisão por 11. Portanto o resto é zero.

iii (13 divide $(10^{1001} - 901)$). De fato, 10^6 deixa resto 1 na divisão por 13 e -901 deixa resto 9, na divisão por 13. Logo, pelo Teorema dos Restos $(10^{1001} - 901))$ deixa o mesmo resto que $((1)^{166} \cdot 10^5 + 9) = 100009$. Assim, o resto também é zero.

1.1.2 Realização e Apoio

Realização:

Apoio:

1.2 Aula 02 - Divisibilidade II

Definição 1.2.1 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 $a|b$ se o r obtido pelo algoritmo de divisão aplicado à a e b é 0, ou seja, se $b = aq$ para algum inteiro q. $\Diamond$

Lema 1.2.2 *Sejam a, b, c, d inteiros. Temos*

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

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

iii ("Transitividade") Se $a|b$ e $b|c$, então $a|c$.

Exemplo 1.2.3 (Olimpíada de Maio 2006). Encontre todos os naturais a e b tais que $a|(b+1)$ e $b|(a+1)$.**Solução**. Pelo Lema **??** ("Limitação"),

$$a|(b+1) \Rightarrow a \leq b+1$$
$$b|(a+1) \Rightarrow b \leq a+1 \Leftrightarrow b-1 \leq a$$

Ou seja,

$$b-1 \leq a \leq b+1,$$

então temos três possibilidades: $a = b-1$ ou $a = b$ ou $a = b+1$.

- Se $a = b-1$, então

$$a|(b-1) \quad \text{e} \quad a|(b+1).$$

Pelo item i do Lema **??**, escolhendo $x = -1$ e $y = 1$ temos

$$a|[(b-1)\cdot(-1) + (b+1)\cdot(1)]$$
$$a|2.$$

Então, $a = 1$ ou $a = 2$. Se $a = 1, b = 2$ e se $a = 2, b = 3$.

- Se $a = b$, então

$$a|a \quad \text{e} \quad a|(a+1),$$

Logo, $a|[(a+1) - a]$. Portanto, $a|1$ e consequentemente $a = 1$ e $b = 1$.

- Se $a = b+1$, isto significa que $b = a-1$. Assim,

$$b|(a-1) \quad \text{e} \quad b|(a+1),$$

logo

$$b|(a+1) - (a-1).$$

Portanto, $b|2$, então $b = 1, a = 2$ ou $b = 2, a = 3$.

O conjunto de todas as soluções: $\{(1,2),(2,3),(1,1),(2,1),(3,2)\}$ $\square$

Proposição 1.2.4 (PTOM)(Critério de divisibilidade por 2). *Seja n um número inteiro com k dígitos na base* 10*:*

$$n = r_k r_{k-1} \dots r_1 r_0,$$

então $2|n$ *se, e somente se,* $2|r_0$.

Referências BibliográficasReferências Bibliográficasx:references:referencias

[1] Notas de aula de Teoria dos Números do POTI