Material Teórico - Módulo Aritmética dos Restos

Divisibilidade e Resto - Parte 1

Tópicos Adicionais

Autor: Ulisses Lima Parente
Revisor: Prof. Antonio Caminha M. Neto

12 de dezembro de 2022

No módulo "Algoritmo de Euclides Estendido", com o auxílio do Teorema de Eudoxius, demonstramos o Algoritmo da Divisão, teorema que será o ponto de partida deste módulo. Pela importância desse teorema para o módulo, refaremos a demonstração que foi feita lá. Caso você já tenha lido a demonstração, pode pular diretamente para os exemplos que a sucedem.

Teorema 1 (Eudoxius). *Dados a e b inteiros, com $b > 0$, tem-se que ou a é múltiplo de b ou está localizado entre dois múltiplos consecutivos de b. De outro modo, dados a e b inteiros, com $b > 0$, existe q inteiro tal que*

$$bq \leq a < b(q+1).$$

Prova. Suponha que $a \geq 0$ (o caso $a < 0$ pode ser tratado de forma análoga) e considere o número racional $\frac{a}{b}$.

O fato de o conjunto $\mathbb{N}$ dos números naturais ser ilimitado superiormente garante a existência de um natural maior que $\frac{a}{b}$. Dentre todos esses naturais, existe um que é o menor possível; chame-o de n. Então, $\frac{a}{b} < n$ é verdade, mas a minimalidade de n garante que $\frac{a}{b} < n-1$ é falso. Portanto, $\frac{a}{b} \geq n-1$, de modo que

$$n - 1 \leq \frac{a}{b} < n.$$

Chamando $n-1$ de q, temos $n = q+1$ e

$$q \leq \frac{a}{b} < q+1.$$

Multiplicando as desigualdades acima por b, segue finalmente que

$$bq \leq a < b(q+1),$$

conforme desejado. □

Agora, apresentamos uma demonstração para o Algoritmo da Divisão.

Teorema 2 (Algoritmo da Divisão). *Dados inteiros positivos a e b, existem, e são únicos, inteiros q e r tais que*

$$a = bq + r, \text{ com } 0 \leq r < b.$$

Os números inteiros q e r são denominados ***quociente*** *e* ***resto*** *da divisão de a por b, respectivamente.*

Prova. Pelo Teorema de Eudoxius, existe um número inteiro q tal que

$$bq \leq a < b(q+1).$$

Assim:

$$bq \leq a \Longrightarrow 0 \leq a - bq$$

e

$$a < b(q+1) \Longrightarrow a < bq + b \Longrightarrow a - bq < b.$$

Daí, fazendo $r = a - bq$, obtemos

$$a = bq + r,\ 0 \leq r < b.$$

Para provar a unicidade, suponha que q' e r' sejam inteiros tais que

$$a = bq' + r', \text{ com } 0 \leq r' < b.$$

Então

$$bq + r = a = bq' + r' \Longrightarrow b(q - q') = r' - r,$$

de sorte que

$$b|q' - q| = |r' - r|. \tag{1}$$

Logo, $|r' - r|$ é múltiplo de b. Mas veja que

$$r' < b \Longrightarrow r' - r < b - r < b$$

e

$$r < b \Longrightarrow r - r' < b - r' < b.$$

Assim, $|r' - r| < b$, de maneira que $|r' - r|$ é um múltiplo de b tal que $0 \leq |r' - r| < b$. Portanto, a única possibilidade é que $|r' - r| = 0$. Daí, $r' = r$ e, graças a (1), $q' = q$. Desse modo, quociente e resto da divisão de a por b são únicos. □

Continuando, apresentamos algumas aplicações do teorema 2.

Exemplo 3. *Mostre que, dentre três inteiros consecutivos, exatamente um deles é múltiplo de* 3*. Além disso, mostre também que a soma de três inteiros consecutivos é um múltiplo de* 3*.*

Solução. Vamos denotar por n, $n+1$ e $n+2$ os três inteiros consecutivos. Pelo teorema 2, temos que existem q e r (únicos) inteiros tais que $n = 3q + r$, em que $0 \leq r < 3$, ou seja, $r \in \{0,1,2\}$. Assim, temos

- se $n = 3q$, então não há nada a fazer, pois n é múltiplo de 3;
- se $n = 3q+1$, então $n+2 = (3q+1)+2 = 3q+3 = 3(q+1)$, ou seja, $n+2$ é múltiplo de 3;
- se $n = 3q+2$, então $n+1 = (3q+2)+1 = 3q+3 = 3(q+1)$, ou seja, $n+1$ é múltiplo de 3.

Para mostrar que a soma dos três números inteiros consecutivos n, $n+1$ e $n+2$ é um múltiplo de 3, note que se $n = 3q$ então

$$\begin{aligned} n + (n+1) + (n+2) &= 3q + (3q+1) + (3q+2) \\ &= 9q + 3 \\ &= 3(3q+1); \end{aligned}$$

se $n = 3q + 1$, então

$$\begin{aligned} n + (n+1) + (n+2) &= (3q+1) + (3q+2) + (3q+3) \\ &= 9q + 6 \\ &= 3(3q+2) \end{aligned}$$

e, se $n = 3q + 2$, então

$$\begin{aligned} n + (n+1) + (n+2) &= (3q+2) + (3q+3) + (3q+4) \\ &= 9q + 9 \\ &= 3(3q+3). \end{aligned}$$

Assim, obtemos que $n+(n+1)+(n+2)$ é múltiplo de 3. □

Antes de apresentar o próximo exemplo, convém recordar o seguinte

Teorema 4 (Euclides). *O conjunto dos números primos é infinito.*

Prova. Suponha que o conjunto P dos números primos seja finito, digamos, $P = \{p_1,p_2,\ldots,p_r\}$. Agora, considere o número $n = p_1p_2\ldots p_r + 1$. Perceba que $n > p_i$, $\forall i \in \{1,2,\ldots,r\}$, logo, n não é primo. Por outro lado, pelo lema de Euclides, apresentado no módulo "Algoritmo de Euclides Estendido", como $n > 1$ não é primo, existe algum primo p que o divide. Como $p \in P$, existem um inteiro $i \in \{1,2,\ldots,r\}$ tal que $p = p_i$. Portanto, $p_i \mid (p_1p_2\ldots p_r + 1)$. Agora, veja que $p_i \mid p_1p_2\ldots p_r$, de sorte que p_i divide a diferença $(p_1p_2\ldots p_r + 1) - p_1p_2\ldots p_r$, isto é, $p_i \mid 1$. Isso, obviamente, é uma contradição, que vem de termos suposto que P fosse um conjunto finito. Desse modo, concluímos que o conjunto dos números primos é infinito. □

Dois números primos p e q, com $p < q$, são denominados **primos gêmeos** se $q = p + 2$; três números primos p, q e r, com $p < q < r$, são denominados **primos trigêmeos** se $q = p + 2$ e $r = p + 4$. São exemplos de primos gêmeos os pares 3 e 5, 5 e 7, 11 e 13, 17 e 19, etc. Por outro lado, o trio 3, 5 e 7 é um exemplo de primos trigêmeos.

Observação 5. *O maior par de primos gêmeos conhecido foi descoberto em* 2016*. Cada um dos primos que formam esse par possui* 388.342 *algarismos. Uma conjectura matemática famosa, conhecida como a "Conjectura dos Primos Gêmeos", afirma que a quantidade de pares de primos gêmeos é infinita. Até hoje, não há uma demonstração para essa conjectura, mas também não há um argumento que prove que ela não é verdadeira. Entretanto, em* 2013*, o matemático chinês Yitang Zhang mostrou a existência de um número N tal que existem infinitos pares de números primos cuja diferença é N. Perceba que a Conjectura dos Primos Gêmeos seria o caso $N = 2$ do teorema de Y. Zhang. O argumento de Zhang também mostrou que o número N pode ser tomado menor*

do que 70 *milhões. Trabalhos posteriores mostraram que o teorema é verdadeiro para* $N = 246$*. Por outro lado, o trio* 3, 5 *e* 7 *é o único trio de primos trigêmeos, como veremos no próximo exemplo.*

Exemplo 6. *Os números* 3, 5 *e* 7 *são os únicos primos trigêmeos.*

Solução. De fato, suponha que p, $p+2$ e $p+4$ sejam primos ímpares consecutivos. Repetindo o raciocínio do exemplo anterior, existem (únicos) inteiros q e r tais que $p = 3q+r$, em que $0 \leq r < 3$. Daí, ocorre uma das seguintes possibilidades:

- $p = 3q$, o que implica $q = 1$, pois p é primo. Logo, $p = 3$, $p + 2 = 5$ e $p + 4 = 7$;
- $p = 3q + 1$, logo, $p + 2 = (3q + 1) + 2 = 3q + 3 = 3(q + 1)$. Daí, $p + 2$ é um número primo que é múltiplo de 3. Assim, $p + 2 = 3$ e, portanto, $p = 1$. Mas isso é uma contradição, pois p é primo.
- $p = 3q + 2$, o que acarreta $p + 4 = (3q + 2) + 4 = 3q + 6 = 3(q + 2)$. Repetindo o raciocínio do item anterior, obtemos $p + 4 = 3$. Daí, $p = -1$, o que é uma contradição.

Desse modo, concluímos que os únicos primos trigêmeos são 3, 5 e 7. □

Embora existam infinitos números primos, assim como existem infinitos pares de primos cuja diferença vale 246, podemos encontrar "saltos" arbitrariamente grandes na sequência dos números primos. Veja o exemplo abaixo.

Exemplo 7. *Qualquer que seja o inteiro positivo* k*, todos os números da sequência*

$$(k+1)!+2,\ (k+1)!+3,\ \ldots,\ (k+1)!+k,\ (k+1)!+(k+1)$$

são compostos.

Solução. Uma vez que $(k+1)! = (k+1)\cdot k\cdot(k-1)\cdot\ldots\cdot 3\cdot 2$, temos que $(k+1)!$ é divisível por cada um dos números do conjunto $\{2,3,\ldots,k,k+1\}$. Desse modo, $2 \mid [(k+1)!+2]$, $3 \mid [(k+1)!+3]$, e assim por diante, ou seja, $i \mid [(k+1)!+i]$, $\forall i \in \{2,3,\ldots,k,k+1\}$. Portanto, os números da sequência

$$(k+1)!+2,\ (k+1)!+3,\ \ldots,\ (k+1)!+k,\ (k+1)!+(k+1)$$

são, de fato, todos compostos. □

Exemplo 8. *Se p, $4p^2+1$ e $6p^2+1$ são números primos, mostre que $p=5$.*

Solução. Quando dividimos p por 5, obtemos cinco possíveis restos: 0, 1, 2, 3 ou 4. Se fosse $p = 5q+1$, então teríamos

$$\begin{aligned} 4p^2+1 &= 4(5q+1)^2+1 \\ &= 4\left(25q^2+10q+1\right)+1 \\ &= 100q^2+40q+4+1 \\ &= 100q^2+40q+5 \\ &= 5\left(20q^2+8q+1\right). \end{aligned}$$

Assim, $4q^2+1$ não seria primo, pois seria um múltiplo de 5 maior que 5. Se fosse $p = 5q+2$, então

$$\begin{aligned} 6p^2+1 &= 6(5q+2)^2+1 \\ &= 6\left(25q^2+20q+4\right)+1 \\ &= 150q^2+120q+24+1 \\ &= 150q^2+120q+25 \\ &= 5\left(30q^2+24q+5\right). \end{aligned}$$

Logo, $6q^2+1$ não seria primo, pois seria um múltiplo de 5 maior que 5. Se fosse $p = 5q+3$, então

$$\begin{aligned} 6p^2+1 &= 6(5q+3)^2+1 \\ &= 6\left(25q^2+30q+9\right)+1 \\ &= 150q^2+180q+54+1 \\ &= 150q^2+180q+55 \\ &= 5\left(30q^2+36q+11\right), \end{aligned}$$

novamente um múltiplo de 5 maior que 5. Finalmente, se $p = 5q + 4$, então

$$\begin{aligned} 4p^2 + 1 &= 4(5q + 4)^2 + 1 \\ &= 4\left(25q^2 + 40q + 16\right) + 1 \\ &= 100q^2 + 160q + 64 + 1 \\ &= 100q^2 + 160q + 65 \\ &= 5\left(20q^2 + 32q + 13\right). \end{aligned}$$

Também nesse caso, $4q^2 + 1$ não seria primo.

Assim, concluímos que a única alternativa para a qual p, $4p^2 + 1$ e $6p^2 + 1$ podem ser primos é $r = 0$, ou seja, $p = 5q$. Desse modo, como p é primo, temos $p = 5$, $4p^2 + 1 = 101$ e $6p^2 + 1 = 151$. Por fim, não é difícil verificar que 101 e 151 são realmente primos. □

Exemplo 9. *Mostre que existem infinitos primos que deixam resto* 5 *quando divididos por* 6*. Em outras palavras, existem infinitos primos da forma* $6q + 5$*.*

Prova. Iniciamos observando que, ao dividir um número inteiro qualquer por 6, os possíveis restos formam o conjunto {0,1,2,3,4,5}. Assim, todo número inteiro pode ser escrito de exatamente uma das seguintes formas: $6q$, $6q + 1$, $6q + 2$, $6q + 3$, $6q + 4$ ou $6q + 5$.

Observamos, ainda, que os números inteiros maiores que 2 que podem ser escritos de uma das formas $6q = 2 \cdot 3q$, $6q + 2 = 2(3q + 1)$ e $6q + 4 = 2(3q + 2)$ são compostos — pois são múltiplos de 2 —, assim como os inteiros maiores que 3 que podem ser escritos da forma $6q + 3 = 3(2q + 1)$ — pois são múltiplos de 3.

Portanto, para qualquer número primo p maior do que 3, temos que $p = 6q + 1$ ou $p = 6k + 5$.

Agora, vamos supor que existe somente uma quantidade finita de primos da forma $6q+5$, digamos, $p_1 = 5, p_2, p_3, \ldots, p_r$, e considere o número $n = 6p_2p_3 \ldots p_r + 5$.

Veja que n é ímpar, logo, possui apenas fatores primos ímpares. Contudo, $p_1 = 5 \nmid n$ (pois $5 \nmid 6p_2p_3 \ldots p_r$) e tampouco nenhum dos primos p_i, com $2 \leq i \leq r$, divide n (pois,

do contrário, p_i dividiria a diferença $n - 6p_2p_3 \dots p_r$, isto é, p_i dividiria 5; logo, teríamos $p_i = 5$, o que, por sua vez, seria uma contradição). Evidentemente, também temos que $3 \nmid n$.

Portanto, pelo Lema de Euclides, n poderia ser escrito como um produto de primos da forma $6q + 1$. Entretanto, o produto de números da forma $6q + 1$ também tem é da forma $6q + 1$; realmente, se q_1 e q_2 são inteiros positivos, então

$$\begin{aligned}(6q_1 + 1)(6q_2 + 1) &= 36q_1q_2 + 6q_1 + 6q_2 + 1 \\ &= 6(6q_1q_2 + q_1 + q_2) + 1 \\ &= 6q_0 + 1,\end{aligned}$$

em que $q_0 = 6q_1q_2 + q_1 + q_2 \in \mathbb{Z}$.

Chegamos, então, a uma contradição: por um lado, $n = 6q+5$; por outro, $n = 6q'+1$. Concluímos, assim, que existem infinitos primos da forma $6q + 5$. □

Observação 10. *O exemplo 9 é um caso particular de um importante teorema sobre a distribuição dos números primos ao longo dos naturais, conhecido como Teorema de Dirichlet. Ele afirma que, se a e b são números inteiros positivos primos entre si, isto é,* $\text{mdc}\,(a,b) = 1$*, então a progressão aritmética $a_n = a + nb$ contém infinitos primos.*

Dicas para o Professor

Sugerimos que sejam utilizadas duas sessões de 50min para expor o conteúdo deste material. Se os alunos já estiverem familiarizados com o Algoritmo da Divisão, esse tópico pode ser omitido e a aula pode ser iniciada a partir dos exemplos.

Recomendamos que os professores deixem os alunos refletirem sobre os exemplos apresentados por alguns minutos, antes de explicarem as soluções. Ressaltamos a importância de que os alunos tentem encontrar as soluções por meios prórpios. Por outro lado, ainda que eles não as encontrem, ou apresentem uma solução errada, esse processo é fundamental para a aprendizagem.

Idealmente, apresente aos alunos outros exemplos que possam ser resolvidos com a mesma ideia apresentada no exemplo 6. Uma possibilidade é pedir que encontrem p, sabendo que p, $p+10$ e $p+14$ são números primos. Outro caso particular do Teorema de Dirichlet que pode ser apresentado aos alunos é o seguinte: mostre que existem infinitos primos que deixam resto 3 quando divididos por 4; ou seja, mostre que há infinitos primos da forma $4q + 3$.

A demonstração do Teorema de Dirichlet foge do escopo desse material. Contudo, para o leitor interessado, o caso $a = 1$ admite uma demonstração mais simples, que pode ser lida na referência [1]; para o caso geral, veja [2].

Sugestões de Leitura Complementar

1. A. C. Muniz Neto. *Tópicos de Matemática Elementar, Volume 6: Polinômios*. Rio de Janeiro, SBM, 2016.

2. F. B. Martínez, C. G. Moreira, N. Saldanha e E. Tengan. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*. Rio de Janeiro, SBM 2018.