POLOS OLÍMPICOS DE TREINAMENTO INTENSIVO

Teoria de Números

Notas de Aula

Nível 2 - UFPR

Raquel A. Aita e
Eduardo C. Araujo

1 Divisibilidade

Nesta primeira seção, introduziremos conceitos mais simples, porém importantes, que serão frequentemente utilizados no decorrer de todo o curso. Inicialmente, iremos manter a atenção em propriedades e resultados acerca dos números inteiros positivos, conjunto que será denotado por $\mathbb{Z}^+$. O caso negativo será tratado mais adiante.

Dados números inteiros genéricos a e b, já conhecemos a operação de divisão: $a \div b$. Obtemos desta dois inteiros positivos - resto r e quociente q. Podemos então escrever o número a como

$$a = bq + r$$

Acerca dessa notação, podemos enunciar nosso primeiro resultado:

Teorema 1 (Algoritmo da Divisão)**.** *Para quaisquer inteiros positivos a e b, o quociente q e resto r da divisão de a por b são únicos, desde que se fixe $r < b$. Equivalentemente, existe única forma de escrever $a = bq + r$, para r estritamente menor que b.*

Um *teorema* é uma afirmação válida sobre certas circunstâncias, chamadas *hipóteses* (nesse caso, a e b devem ser inteiros positivos). Satisfeitas as condições, o resultado é sempre válido, sem exceções. Porém, todo teorema deve ser acompanhado de uma *demonstração*. É essa prova rigorosa uma das principais características da Matemática, que faz com que ela seja sólida e todos os seus resultados sejam concretos. Para o teorema anterior, uma das demonstrações é a seguinte:

Demonstração. *Sejam a e b como solicitados. Se q e r são únicos, vamos mostrar que não pode existir um resto $\hat{r}$ diferente do primeiro, satisfazendo $\hat{r} < b$. Suponha que exista $\hat{r} \neq r$, então como ambos são menores do que b por hipótese, sabemos que $0 < r - \hat{r} < b$. Mas $a = bq + r = b\hat{q} + \hat{r}$, então $bq + (r - \hat{r}) = b\hat{q}$. Note então que $(r - \hat{r})$ deve ser divisível por b, ao mesmo tempo que é menor que ele, o que é impossível. Assim, a suposição $r \neq \hat{r}$ era incorreta, e necessariamente $r = \hat{r}$, o que implica $q = \hat{q}$. Portanto, q e r são únicos.*

A tática usada acima é chamada *demonstração por absurdo* e é uma das mais famosas na matemática, da qual faremos uso frequentemente. Outras abordagens serão apresentadas no decorrer do curso. No começo, é naturalmente complicado compreender o passo a passo de uma demonstração. Recomendamos que o aluno se concentre no resultado do teorema, mas que, aos poucos, busque uma compreensão maior da prova, de maneira que lentamente se sinta mais confortável.

Do Teorema 1, agora sabemos que podemos representar qualquer número natural a de maneira única na forma $a = bq + r$, para qualquer b conveniente. Note que a unicidade é completamente essencial aqui, pois caso contrário um número poderia ser escrito de duas formas diferentes, o que complicaria nossa análise. Observe o exemplo a seguir:

Exemplo 1. *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. *À primeira vista, pode parecer uma boa ideia chutar valores até encontrar um que satisfaça as condições. Porém, uma solução é facilmente encontrada utilizando o Algoritmo de Euclides; note que* $n+1$ *deixará resto* 0 *na divisão por 10, 9 e 8 (visto que o resto é estritamente menor que o divisor).*
Assim, é mais fácil estudar $n+1$ *quando escrito na forma* $n+1 = bq + r$. *Como* $r = 0$ *quando* $q = 10, 9, 8$, *uma das possíveis soluções é* $n + 1 = 10 \cdot 9 \cdot 8 + 0$. *Ou seja,* $n = 719$.

Reiteramos que todas as soluções são *propostas* e que o aluno deve sentir-se livre para buscar outras maneiras de resolver o mesmo problema, usando ferramentas distintas.

Após definir o algoritmo da divisão, podemos nos questionar: como ele se comporta quando junto de outras operações? O que acontece ao dividir uma soma? E um produto? O seguinte teorema nos dará um simples porém poderoso resultado, e responderá essas dúvidas.

Teorema 2 (Teorema dos Restos)**.** *Sejam* r_1 *e* r_2 *os restos de* $a_1 \div b$ *e* $a_2 \div b$, *respectivamente. Então,*

1. $(a_1 + a_2) \div b$ *deixa resto* $r_1 + r_2$
2. $(a_1 \times a_2) \div b$ *deixa resto* $r_1 \times r_2$

Demonstração. *Em breve.*

Com este resultado em mãos, podemos resolver questões que antes pareciam impossíveis.

Exemplo 2. *Qual o resto que o número* 4^{2019} *deixa ao ser dividido por* 3*?*

Solução. *Primeiramente, note que* $4 \div 3$ *possui resto 1. Do* ***Teorema dos Restos****, segue que* $(4 \cdot 4) \div 3 = 4^2 \div 3$ *deixa resto* $1 \cdot 1 = 1^2$, $(4^2 \cdot 4) \div 3 = 4^3 \div 3$ *tem resto* $1^2 \cdot 1 = 1^3$, *e assim sucessivamente. Concluímos portanto que* $4^{2019} \div 3$ *deixa resto* $1^{2019} = 1$.

Podemos também unir este resultado com outras técnicas de demonstração. No exercício abaixo, utilizaremos a *análise caso a caso* do problema, muito usada em problemas olímpicos. A estratégia consiste em dividir um caso complicado em partes mais simples.

Exemplo 3. *Qual o resto de* $n^3 + 2n$ *na divisão por* 3*?*

Solução. *Denote por* r *o resto de* $n \div 3$. *Como* $2 \div 3$ *tem resto* 2, *segue do* ***Teorema dos Restos*** *que* $(2 \cdot n) \div 3$ *tem resto* $2 \cdot r$. *Analogamente,* $n^3 \div 3$ *deixa resto* r^3. *Então,* $(n^3 + 2n) \div 3$ *possui resto* $r^3 + 2r$. *Como os possíveis valores para* r *são 0, 1 e 2 (lembre-se que estamos dividindo por 3), analisemos cada um dos casos:*

- *se* $r = 0$, *o resto será* $0^3 + 2 \cdot 0 = 0$, *logo* $n^3 + 2n$ *é divisível por* 3.
- *se* $r = 1$, *o resto será* $1^3 + 2 \cdot 1 = 3$, *que é múltiplo de* 3, *logo* $n^3 + 2n$ *é divisível por* 3.
- *se* $r = 2$, *o resto será* $2^3 + 2 \cdot 2 = 12$, *que é múltiplo de* 3, *logo* $n^3 + 2n$ *é divisível por* 3.

Logo, $n^3 + 2n$ *é divisível por 3 para qualquer* n.

Observe que ao obtermos $r = 0$, necessariamente a é um múltiplo de b. Definimos este caso da seguinte maneira:

Definição. *Dados dois inteiros a e b, com $b \neq 0$, dizemos que b divide a e escrevemos $a|b$ (leia-se: a é divisível por b), se existe um número q tal que $a = bq$, ou seja, $r = 0$.*

Novamente, podemos nos questionar como se comporta a divisibilidade em outras condições.

Teorema 3 (Propriedades da Divisibilidade)**.** *Sejam a, b, c, d números inteiros. Então:*

1. *Se a e b são divisíveis por d, então $ax + by$ também o é, para quaisquer x e y inteiros;*
2. *(Limitação) Se d divide a, então $a = 0$ ou d é menor ou igual a a;*
3. *(Transitividade) Se a divide b e b divide c, então a também divide c.*

Observe que, com a notação introduzida, podemos escrever as mesmas propriedades da seguinte maneira:

1. Se $a|d$ e $b|d$, então $ax + by|d$, para todo $x, y \in \mathbb{Z}^+$
2. (Limitação) Se $a|d$, então $a = 0$ ou $d \leq a$
3. (Transitividade) Se $b|a$ e $c|b$, então $c|a$

No começo, a notação matemática pode ser um complicador. Mas, com o tempo, ela se torna uma grande aliada pela economia de tempo e simplicidade na hora de escrever. Introduziremos pouco a pouco os símbolos novos para facilitar a adaptação do aluno.

Com as propriedades enunciadas, fica clara a grande vantagem de dividir um número por um de seus divisores, já que isto elimina o resto. É claro que sempre é possível decidir se um número é divisível por outro executando a divisão e analisando seu resto. Porém, muitas vezes não estamos interessados no quociente em si, de maneira que o processo pode ser demorado e não compensar. Para nos auxiliar com esse problema, utilizamos os *Critérios de Divisbilidade*, que são regras que nos permitem determinar rapidamente se um número é múltiplo de outro.

O critério mais conhecidos, sem sombra de dúvida, é o do número 2: sabemos que a é divisível por 2 se e somente se a for par. Mas existem diversos outros, nem tão conhecidos porém igualmente práticos. Enunciamos alguns deles a seguir:

- **Critério de divisibilidade por 2:**
  Um número N é divisível por 2 quando seu algarismo das unidades for par.
- **Critério de divisibilidade por 3:**
  Um número N é divisivel por 3 se a soma dos seus algarismos também for divisível por 3.
- **Critério de divisibilidade por 4:**
  Um número N é divisível por 4 quando seus dois últimos algarismos formam um número divisível por 4, ou seja, quando o número formado pelos algarismos das dezenas e das unidades de N é divisível por 4.
- **Critério de divisibilidade por 5:**
  Um número N é divisível por 5 se seu algarismo das unidades é 0 ou 5.
- **Critério de divisibilidade por 6:**
  Um número N é divisível por 6 quando é simultaneamente divisível por 2 e 3.

- **Critério de divisibilidade por 7:**
  Um número N é divisível por 7 se, ao apagar seu último dígito, multiplicá-lo por 2 e subtraí-lo do número que restou, também seja divisível por 7. Esse critério é utilizado indutivamente.

- **Critério de divisibilidade por 8:**
  Um número N é divisível por 8 quando seus três últimos algarismos formam um número divisível por 8, ou seja, quando o número formado pelos algarismos das centenas, dezenas e unidades de N é divisível por 8.

- **Critério de divisibilidade por 9:**
  Um número N é divisível por 9 se a soma dos seus algarismos for um número divisível por 9.

- **Critério de divisibilidade por 10:**
  Um número N é divisível por 10 se o seu alagarismo das unidades for o 0.

- **Critério de divisibilidade por 11:**
  Um número N é divisível por 11 quando a diferença não negativa entre a soma dos algarismos de ordem ímpar e a soma dos algarismos de ordem par for um número divisível por 11.

Continua...