MATEMÁTICA

FRENTE: MATEMÁTICA IV

PROFESSOR(A): ISAAC LUÍS

EAD – ITA/IME

AULAS 01 A 04

ASSUNTO: O PRINCÍPIO DE INDUÇÃO MATEMÁTICA

Resumo Teórico

Introdução

Neste nosso primeiro encontro, estudaremos uma ferramenta de extrema importância no que diz respeito a demonstrações de proposições e teoremas associados, num certo sentido, ao conjunto dos números inteiros (Z): a indução matemática. Para começarmos, vejamos algumas definições.

Seja S um subconjunto de Z (isto é, $S \subset Z$). Dizemos que $s_0 \in S$ é o elemento mínimo de S (ou, simplesmente, o mínimo de S) se $s_0 \leq s$, para todo $s \in S$. Nesse caso, escrevemos $s_0 = \text{mín}S$. De modo análogo, define-se o elemento máximo (ou, simplesmente, o máximo) de um conjunto. Diremos, ainda, que S é limitado inferiormente se existir um inteiro **m** tal que $m \leq s$, para todo $s \in S$.

De posse das definições acima, enunciaremos o seguinte:

Axioma (Princípio da boa ordenação): Todo subconjunto não vazio de inteiros não negativos possui mínimo.

O axioma acima tem uma série de implicações (veja os exercícios 1 e 2, por exemplo). Com ele, demonstraremos um teorema que nos servirá de base para enunciarmos o primeiro princípio de indução.

Teorema: Sejam **m** um inteiro e S um subconjunto de inteiros maiores do que ou iguais a **m** tal que:

i) $m \in S$;
ii) Se o inteiro $k \geq m$ pertence a S, então $(k + 1)$ também pertence a S.

Nessas condições, S é o conjunto de todos os inteiros maiores do que ou iguais a **m**.

Prova. Suponha, por absurdo, que exista algum inteiro maior do que ou igual a **m** que não pertença a S. Nesse caso, o conjunto

$$S' = \{n \in Z \mid n \geq m;\ n \notin S\}$$

é não vazio. Daí, conforme o Exercício 2, S′ tem mínimo s_0'. Repare que $s_0' > m$, já que, por hipótese, $m \in S$. Assim, $s_0' - 1 \geq m$. Evidentemente, $s_0' - 1$ não pertence a S′, uma vez que $s_0' - 1 < s_0'$. Daí, $s_0' - 1$ pertence a S, de modo que, em virtude de ii),

$$(s_0' - 1) + 1 = s_0' \in S,$$

claramente uma impossibilidade.

O Primeiro Princípio de Indução

Uma consequência imediata do teorema que acabamos de provar é o seguinte:

Corolário (Primeiro princípio de indução): Sejam **m** um inteiro e P(n) uma sentença aberta definida sobre o conjunto dos inteiros maiores do que ou iguais a **m** tal que:

i) P(m) é verdadeira;
ii) Se P(k) é verdadeira para algum $k \geq m$, então P (k + 1) também é verdadeira.

Nessas condições, P(n) é verdadeira para todo $n \geq m$.

Prova. Denotemos por V o conjunto verdade de P(n), isto é, V é o conjunto formado por todos os inteiros maiores do que ou iguais a **m** tais que P(n) é verdadeira. Note que, em virtude de i), $m \in V$. Ademais, se o inteiro $n \geq m$ pertence a V, então (n + 1) também pertence a V, por ii). Daí, pelo teorema anterior, V é o conjunto de todos os inteiros maiores do que ou iguais a **m**.

Bom, você certamente irá concordar que, até agora, todas as ideias apresentadas foram expostas com considerável grau de abstração. Estudemos, pois, um exemplo prático, com o intuito de entendermos melhor como se deve aplicar o corolário acima na resolução de problemas.

Exemplo 1

Mostre que a soma dos cubos de três números naturais consecutivos é sempre divisível por 9.

Solução. Considere a sentença aberta

$$P(n):\ 9 \mid n^3 + (n + 1)^3 + (n + 2)^3,$$

definida sobre N. É fácil ver que P(0) é verdadeira, já que

$$0^3 + 1^3 + 2^3 = 9.$$

Agora, suponha P(n) verdadeira para algum $n \geq 0$. Mostraremos que, nesse caso, P(n + 1) também é verdadeira. Com efeito, temos

$$\begin{aligned} &(n + 1)^3 + (n + 2)^3 + (n + 3)^3 = \\ &= (n + 1)^3 + (n + 2)^3 + (n^3 + 9n^2 + 27n + 27) = \\ &= [n^3 + (n + 1)^3 + (n + 2)^3] + 9(n^2 + 3n + 3), \end{aligned}$$

que é divisível por 9, por ser uma soma de múltiplos de 9. Assim, pelo primeiro princípio de indução, P(n) é verdadeira para todo $n \geq 0$, ou seja, P(n) é verdadeira para todo **n** natural.

Vale ressaltar que a prova indutiva dada acima não é, evidentemente, a única alternativa de que dispomos. Podemos, também, dar uma demonstração direta. Note que

$$\begin{aligned} &n^3 + (n+1)^3 + (n+2)^3 = \\ &= n^3 + (n^3 + 3n^2 + 3n + 1) + (n^3 + 6n^2 + 12n + 8) = \\ &= 3n^3 + 9n^2 + 15n + 9 = 3n(n^2 + 5) + 9(n^2 + 1), \end{aligned}$$

e agora, basta analisarmos a parcela $3n(n^2 + 5)$, já que $9(n^2 + 1)$ é claramente um múltiplo de 9. Se **n** é múltiplo de 3, 3n é múltiplo de 9, e nada mais há a fazer. Por outro lado, se **n** não for múltiplo de 3, $n^2 \equiv 1 \pmod 3$, de modo que $n^2 + 5 \equiv 0 \pmod 3$, e assim, $3n(n^2 + 5)$ é múltiplo de 9. Observe que, aqui, a conclusão é ainda mais geral do que o que foi proposto pelo problema – em verdade, a soma dos cubos de três inteiros consecutivos quaisquer é sempre múltipla de 9.

O Primeiro Princípio de Indução – Aplicações

Recorde que, no início desta aula, mencionamos que a indução matemática é uma poderosa técnica para demonstração de proposições e teoremas. Vejamos alguns exemplos.

Exemplo 2

Um número natural é dito triangular se for igual a 1 ou for uma soma de números naturais consecutivos iniciada em 1. Desse modo, a sequência dos números triangulares é a seguinte:

1
1 + 2 = 3
1 + 2 + 3 = 6
1 + 2 + 3 + 4 = 10
....

Mostre que o enésimo número triangular t_n é dado por $\frac{n(n+1)}{2}$.

Solução.
A fórmula acima é claramente verdadeira para n = 1, pois $\frac{1(1+1)}{2} = 1 = t_1$.

Suponha que essa fórmula seja verdadeira para algum $n \geq 1$. Mostremos que, nesse caso, a fórmula também será verdadeira para (n + 1), isto é,

$$t_{n+1} = \frac{(n+1)(n+2)}{2}$$

De fato, note que

$$t_{n+1} = t_n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}.$$

Logo, pelo primeiro princípio de indução, a fórmula é válida para todo **n** natural, $n \geq 1$.
Vários teoremas clássicos da geometria euclidiana plana podem ser provados com argumentos indutivos.

Exemplo 3
A soma dos ângulos internos de um polígono convexo com **n** lados é dada por

$$(n - 2) \times 180°.$$

Prova. É claro que, aqui, $n \geq 3$. No caso do triângulo, temos $(3 - 2) \times 180° = 1 \times 180° = 180°$,

o que é verdadeiro. Suponha que a fórmula seja verdadeira para polígonos convexos com **n** lados, $n \geq 3$. Mostraremos que, nesse caso, a fórmula também é verdadeira para polígonos com (n + 1) lados. Para tanto, consideremos um polígono convexo P cujos vértices consecutivos são $P_1, P_2, P_3, \ldots, P_n$ e $P_{(n+1)}$. Trace a diagonal $\overline{P_1P_n}$, de modo que P fique dividido no polígono convexo P' com **n** lados e o triângulo $P_1P_n\,P_{(n+1)}$. Agora, repare que a soma dos ângulos internos de P corresponde à soma dos ângulos internos de P' com a soma dos ângulos do triângulo supracitado, ou seja,

$$(n - 2) \times 180° + 180° = (n - 2 + 1) \times 180° = [(n + 1) - 2] \times 180°,$$

o que prova a veracidade da fórmula para polígonos com (n+1) lados.

O próximo exemplo é um pouco mais elaborado. Nossa intenção aqui é deixar claro que, em certas situações, a etapa indutiva pode requerer manipulações algébricas e alguns resultados auxiliares.

Exemplo 4

(Pequeno teorema de Fermat) Sejam **a** um inteiro e **p** um primo. Então, $a^p \equiv a \pmod p$.

Prova. Inicialmente, provaremos o seguinte

Lema: $p \mid \binom{p}{j}$, para todo $1 \leq j \leq p - 1$.

Com efeito, temos

$$\binom{p}{j} = \frac{p!}{j!(p-j)!} = \frac{p \times (p-1) \ldots \times (p-j+1)(p-j)!}{j!(p-j)!} \Rightarrow$$

$$\Rightarrow p \times (p-1) \times \ldots \times (p-j+1) = j! \times \binom{p}{j},$$

donde concluímos que $p \mid j! \times \binom{p}{j}$. Como mdc(p, j!) = 1, o resultado segue (veja o exercício 3).

Voltando à prova do teorema, repare que, se p = 2, podemos escrever

$$a^2 - a = a(a - 1),$$

que é um múltiplo de 2, evidentemente. Assim, no que segue, suporemos $p > 2$. Se a = 0 ou a = 1, a congruência em questão é trivialmente verdadeira. Suponha que ela seja verdadeira para algum $a \geq 1$, e mostremos que, nesse caso, ela também será verdadeira para (a + 1). Veja que, pelo binômio de Newton, temos

$$(a+1)^p - (a+1) = \sum_{j=0}^{p} \binom{p}{j} a^j - (a+1) = 1 + a^p + \sum_{j=1}^{p-1} \binom{p}{j} a^j - (a+1) =$$
$$= (a^p - a) + \sum_{j=1}^{p-1} \binom{p}{j} a^j.$$

Em virtude do lema que provamos, segue-se que

$$p \mid \sum_{j=1}^{p-1} \binom{p}{j} a^j;$$

além disso, por hipótese de indução, p | (a^p – a), de maneira que $p \mid (a + 1)^p - (a + 1)$, isto é,

$$(a + 1)^p \equiv a + 1 \ (\text{mod} p).$$

Com isso, falta apenas considerarmos o caso em que **a** é um inteiro negativo e p > 2. Ora, se a < 0, o teorema é válido para (– a), ou seja,

$$(-a)^p = -a^p \equiv -a \ (\text{mod} p) \Rightarrow a^p \equiv a \ (\text{mod} p),$$

encerrando a prova.

Observações Importantes

Como acabamos de ver, algumas provas indutivas carregam consigo uma série de sutilezas. Em certos casos, sequer é possível aplicar a indução matemática. Para entender melhor o que estamos dizendo, considere, por exemplo, o trinômio quadrático

$$n^2 + n + 41,$$

estudado com afinco pelo grande matemático Leonhard Euler. Se, nesse trinômio, substituirmos **n** por qualquer número inteiro pertencente ao conjunto {1, 2, …, 38, 39}, o valor correspondente obtido é sempre um número primo. Intuitivamente, somos levados a considerar, portanto, a possibilidade de que o trinômio em questão assuma sempre valores primos, qualquer que seja **n** natural – o que não procede. De fato, se n = 40, temos

$$40^2 + 40 + 41 = 40 \times (40 + 1) + 41 = 41 \times (40 + 1) = 41^2,$$

que não é primo, evidentemente. Ademais, se **n** é um múltiplo de 41 não nulo, esse trinômio é sempre múltiplo de 41, de modo que há uma infinidade de valores possíveis para **n** tais que $n^2 + n + 41$ não é primo.

Ressaltemos também o fato de que nem sempre uma prova indutiva é a melhor alternativa disponível. Em algumas situações, as demonstrações diretas são mais efetivas e, em certos casos, mais gerais – como no exemplo 1.

O Segundo Princípio de Indução

Veremos agora uma variante do primeiro princípio de indução, às vezes denominada indução forte. Para tanto, provaremos o seguinte

Teorema: Sejam **m** um inteiro e S um subconjunto de inteiros maiores do que ou iguais a **m** tal que:

i) $m \in S$;
ii) Se **k** é um inteiro maior do que ou igual a **m** tal que todo inteiro l, $m \le l \le k$, pertence a S, então (k + 1) pertence a S.

Nessas condições, S é o conjunto de todos os inteiros maiores do que ou iguais a **m**.

Prova. Suponha, por absurdo, que exista algum inteiro maior do que ou igual a **m** que não pertença a S. Nesse caso, o conjunto

$$S' = \{n \in Z \mid n \ge m;\ n \notin S\}$$

é não vazio. Daí, conforme o Exercício 2, S′ tem mínimo s_0'. Repare que $s_0' > m$, já que, por hipótese, $m \in S$. Assim, $s_0' - 1 \ge m$. Agora, note que todo inteiro l verificando $m \le l \le s_0' - 1$ pertence a S. Com efeito, se algum desses inteiros, digamos l′, não pertencesse a S, teríamos $l' \in S'$, com $l' \le s_0' - 1 < s_0' = \text{mín } S'$, o que não é possível. Daí, por ii), segue-se que

$$(s_0' - 1) + 1 = s_0' \in S,$$

claramente uma contradição.

Corolário (Segundo princípio de indução): Sejam **m** um inteiro e P(n) uma sentença aberta definida sobre o conjunto dos inteiros maiores do que ou iguais a **m** tal que:

i) P(m) é verdadeira;
ii) Se **k** é um inteiro maior do que ou igual a **m** e P(l) é verdadeira para todo inteiro **l** verificando $m \le l \le k$, então P(k + 1) também é verdadeira.

Nessas condições, P(n) é verdadeira para todo $n \ge m$.
Prova. Denotemos por V o conjunto verdade de P(n). Note que, em virtude de i), $m \in V$. Agora, se **k** é um inteiro maior do que ou igual a **m** tal que todo inteiro **l**, $m \le l \le k$, pertence a V, temos que P(l) é verdadeira para todo **l** verificando $m \le l \le k$, e daí, em virtude de ii), P(k + 1) é verdadeira, isto é, (k + 1) pertence a V. Logo, pelo teorema anterior, V é o conjunto de todos os inteiros maiores do que ou iguais a **m**.

O Segundo Princípio de Indução – Aplicações

No que segue, apresentamos alguns exercícios envolvendo a utilização do corolário que acabamos de provar.

Exemplo 5:
Mostre que todo número natural maior do que ou igual a 2 pode ser decomposto num produto de números primos.

Solução.
Se n = 2, a conclusão é imediata, já que 2 é, ele próprio, um número primo. Suponha o resultado válido para todo natural **m** verificando $2 \le m \le n$, e provemos que, nesse caso, (n + 1) também poderá ser escrito como produto de primos. De fato, se (n + 1) for primo, nada há a fazer. Se não, (n + 1) possui um divisor d_1 com $2 \le d_1 \le n$, isto é,

$$n + 1 = d_1 d_2,$$

para algum $d_2 \in N^*$. Note que $2 \le d_2 \le n$; daí, pela hipótese indutiva, d_1 e d_2 podem ser escritos como produto de primos, e o mesmo ocorrerá com (n + 1), evidentemente.

É possível provar também que a fatoração de um número natural maior do que ou igual a 2, chamada de decomposição canônica, é única, a menos da ordem dos fatores. A existência de tal decomposição, garantida pelo Exemplo 5, e a unicidade da mesma, constituem o famoso teorema fundamental da aritmética.

Exemplo 6:
A conhecidíssima sequência de Fibonacci (F_n) é definida recursivamente da seguinte maneira

$$\{F_1 = F_2 = 1;\ F_n = F_{n-1} + F_{n-2},\ \forall n \ge 3.$$

Assim, os primeiros termos dessa sequência são 1, 1, 2, 3, 5, 8, 13, 21, 34, 55,... . O teorema de Zeckendorf afirma que todo número natural **n** não nulo pode ser escrito, de modo único (a menos da ordem das parcelas, claro), como soma de números de Fibonacci não consecutivos, sendo essa soma chamada de representação de Zeckendorf de **n**. A representação de Zeckendorf de 2018, por exemplo, é a seguinte

$$2018 = 2 + 8 + 34 + 377 + 1597.$$

Mostraremos que todo número natural **n** não nulo admite uma representação de Zeckendorf (a unicidade da representação é deixada como exercício). É claro que esse resultado é válido para 1, 2 e 3, já que esses números são, eles próprios, números de Fibonacci. Suponha o resultado válido para todo natural **m**, com $1 \le m \le n$. Se $(n + 1)$ for um número de Fibonacci, nada a fazer. Se não, seja F_k o maior número de Fibonacci que não excede $(n + 1)$. Observe que, como $n + 1 \ge 2$, temos $k \ge 2$. Considere $N = (n + 1) - F_k$. Desde que

$$1 \le N \le n,$$

N, por hipótese de indução, possui representação de Zeckendorf. Por outro lado, temos

$$n + 1 < F_{k+1} = F_k + F_{k-1} \Rightarrow N = (n + 1) - F_k < F_{k-1},$$

donde concluímos que F_{k-1} não está presente na representação de Zeckendorf de N. Logo, $(n + 1)$ também possui representação de Zeckendorf, posto que $n + 1 = N + F_k$.

Exercícios

01. Seja **m** um inteiro tal que $0 \le m \le 1$. Prove que $m = 0$ ou $m = 1$. Mais geralmente, mostre que, se **n** é um inteiro, e **m** é um inteiro verificando $n \le m \le n + 1$, então $m = n$ ou $m = n + 1$.

02. Prove que todo conjunto não vazio de inteiros limitado inferiormente possui mínimo.

03. Sejam **a**, **b** e **c** inteiros não nulos. Mostre que, se $c \mid ab$ e $mdc(a,c) = 1$, então $c \mid b$. Em seguida, utilize esse fato para concluir que, se **p** é um primo que divide o produto $x_1 x_2$, com x_1 e x_2 inteiros, então $p \mid x_1$ ou $p \mid x_2$. Conclua também que, se y_1, y_2, ... e y_n são inteiros tais que

$$p \mid \prod_{i=1}^{n} y_i,$$

então $p \mid y_j$, para algum $1 \le j \le n$.

04. Sejam **a** e **b** inteiros não nulos tais que $mdc(a, b) = 1$. Mostre que $mdc(a^n,b^n) = 1$, para todo **n** natural.

05. Sejam **a**, **b** e **n** inteiros, com $n \ne 0$. Mostre que, se $a \equiv b \pmod{n}$, então $a^m \equiv b^m \pmod{n}$, para todo **m** natural.

06. Sejam **a** e **b** inteiros distintos. Mostre que $(a - b) \mid (a^n - b^n)$, qualquer que seja **n** natural.

07. Seja **n** um número natural. Mostre que existem **x** e **y** naturais tais que $x^2 - y^2 = n^3$.

08. Mostre que

$$\prod_{i=0}^{n} \cos(2^i x) = \frac{sen(2^{x+1}x)}{2^{n+1} senx},$$

para todo **n** natural e $x \ne k\pi$, com $k \in \mathbb{Z}$.

09. Seja A um conjunto com **n** elementos. Prove, por indução, que o número de subconjuntos de A é dado por 2^n.

10. Mostre, por indução, a validade da seguinte fórmula:

$$\sum_{i=1}^{n} (i \times i!) = (n+1)! - 1$$

11. (Teorema de Plutarco) Seja **n** um número natural não nulo. Mostre que **n** é um número triangular se, e somente se, $8n + 1$ é um quadrado perfeito.

12. Mostre que não existe polinômio p(x), não constante, com coeficientes inteiros, tal que p(n) seja primo, para todo **n** natural não nulo. (Perceba que esse resultado tem forte conexão com o trinômio de Euler estudado acima: $n^2 + n + 41$).

13. Considere a matriz

$$A = [\cos\theta \ sen\theta \ - sen\theta \ \cos\theta].$$

Mostre que

$$A^n = [\cos(n\theta) \ sen(n\theta) \ - sen(n\theta) \ \cos(n\theta)],$$

para todo **n** natural não nulo.

14. (Fórmula de Binet) Prove que o enésimo termo F_n da sequência de Fibonacci é dado por

$$\frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}},$$

para todo $n \ge 1$. Em seguida, mostre que

$$\frac{F_{n+1}}{F_n} = \frac{1+\sqrt{5}}{2}.$$

15. Conclua a demonstração do teorema de Zeckendorf, isto é, prove que, se **n** é um natural não nulo, a representação de Zeckendorf de **n** é única.

GABARITO									
01	02	03	04	05	06	07	08	09	10
–	–	–	–	–	–	–	–	–	–
11	12	13	14	15					
–	–	–	–	–					

– Demonstração.

SUPERVISOR/DIRETOR: MARCELO PENA – AUTOR: ISAAC LUÍS
DIG.: SAMUEL – 11/09/18 – REV.: TEREZA