Actividade Formativa 2

Exemplo de Resolução

1. Uma fracção $\frac{a}{b}$ diz-se irredutível se a e b são números primos entre si. Ou seja e de um modo equivalente, se o único divisor comum a a e b é a unidade.

Suponhamos então que existe um $m \in \mathbb{N}$ não nulo tal que

$$m \,|\, (21n+4),\ m \,|\, (14n+3)$$

Nestas condições e por linearidade tem-se que

$$m \,|\, \underbrace{(3(14n+3)-2(21n+4))}_{=1},$$

pelo que $m = 1$.

2. Case Base: $\mathbf{n = 1}$. Tem-se

$$\frac{b^1 - a^1}{b-a} = 1 = b^0 a^0,$$

o que prova que o caso base verifica-se.

Hipótese de indução: Dado um número natural $n \geq 1$, qualquer, suponhamos que

$$\frac{b^n - a^n}{b-a} = \sum_{i=0}^{n-1} b^i a^{n-i-1}.$$

Tese de indução:

$$\frac{b^{n+1} - a^{n+1}}{b-a} = \sum_{i=0}^{n} b^i a^{n-i}.$$

Para se provar a tese de indução observe-se que

$$\frac{b^{n+1} - a^{n+1}}{b-a} = \frac{(b^n - a^n)b + (b-a)a^n}{b-a} = b\frac{b^n - a^n}{b-a} + a^n,$$

o que permite concluir, por aplicação da hipótese de indução, que

$$\begin{aligned} \frac{b^{n+1} - a^{n+1}}{b-a} &= b\sum_{i=0}^{n-1} b^i a^{n-i-1} + a^n = \sum_{i=0}^{n-1} b^{i+1} a^{n-(i+1)} + a^n \\ &= \sum_{j=1}^{n} b^j a^{n-j} + a^n = \sum_{j=0}^{n} b^j a^{n-j}, \end{aligned}$$

onde na penúltima igualdade se efectuou a mudança de variável $j = i + 1$. Fica assim provada a tese de indução.

Pelo método de indução matemática, podemos assim concluir que, para qualquer número natural $n \geq 1$,

$$\frac{b^n - a^n}{b - a} = \sum_{i=0}^{n-1} b^i a^{n-i-1}.$$

3. Relativamente ao exercício anterior, note-se que para quaisquer $a, b \in \mathbb{Z}$

$$\sum_{i=0}^{n-1} b^i a^{n-i-1}$$

é um número inteiro. Ou seja, atendendo à definição de divisor de um número, o exercício 2 prova, em particular, que dados $a, b \in \mathbb{Z}$, $a \neq b$,

$$(a - b) \,|\, (a^k - b^k), \quad \forall\, k \in \{1, 2, \ldots\}. \tag{1}$$

Assim:

3.1.

3.1.1. Pela propriedade transitiva (Lema 1.1 Propriedade (iii)) tem-se para todo o $k \in \{1, 2, \ldots\}$

$$m \,|\, (a - b),\ (a - b) \,|\, (a^k - b^k) \implies m \,|\, (a^k - b^k),$$

sendo o resultado ainda verdadeiro para $k = 0$.

3.1.2. Suponhamos que o polinómio p é da forma

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0, \quad n \geq 1,\ a_i \in \mathbb{Z},\ i = 0, 1, \ldots, n.$$

Logo, $p(a) - p(b)$ é dado por

$$p(a) - p(b) = a_n(a^n - b^n) + a_{n-1}(a^{n-1} - b^{n-1}) + \ldots + a_2(a^2 - b^2) + a_1(a - b),$$

resultando o pretendido por linearidade (Lema 1.1 Propriedade (i)) e por (1).[1]

3.1.3. De acordo com a alínea 3.1.1, para quaisquer $a, b \in \mathbb{Z}$, $a \neq b$, tem-se

$$m \,|\, (a - b) \implies m \,|\, (a^k - b^k).$$

Em particular, este resultado é válido substituindo $b \in \mathbb{Z}$ por $-b \in \mathbb{Z}$ e considerando k um qualquer número natural ímpar. Dado que para k ímpar, $(-b)^k = (-1)^k b^k = -b^k$, obtém-se neste caso

$$m \,|\, (a + b) \implies m \,|\, (a^k + b^k).$$

[1] Naturalmente para o caso de um polinómio de grau 0 tem-se sempre $p(a) - p(b) = 0$ e, portanto, $a - b \neq 0$ é um divisor de $p(a) - p(b)$.

3.2. Para se provar que o resultado da alínea 3.1.3 é falso para k um número natural par, basta apresentar um contra-exemplo.
Considere-se, por exemplo, $a = 5$, $b = 7$, $m = 3$ e $k = 2$. Tem-se que $3 \mid (a+b)$, $a+b = 12$, mas o 3 não divide $a^2 + b^2 = 74$.

4.

4.1. Atendendo ao Exercício 4.3 sobre Divisibilidade e ao facto de $\text{mdc}(a, b)$ ser um divisor de a e de b tem-se

$$\text{mdc}\left(\frac{a}{\text{mdc}(a,b)}, \frac{b}{\text{mdc}(a,b)}\right) = \frac{1}{\text{mdc}(a,b)}\text{mdc}(a,b) = 1.$$

4.2. Uma vez que $\text{mdc}(a, b) \mid a$, $\text{mdc}(a, b) \mid b$, a e b podem-se escrever na forma $a = 15m$, $b = 15n$, $m, n \in \mathbb{N}$. Deste modo

$$90 = a + b = 15(m + n) \implies m + n = 6.$$

Por outro lado, de acordo com a alínea anterior, $\text{mdc}(m, n) = 1$. Deste modo, esta condição exclui de imediato os casos $m = n = 3$, $m = 2$ e $n = 4$, ou $m = 4$ e $n = 2$, sendo os únicos pares (m, n) de números inteiros positivos possíveis

$$(m, n) = (1, 5) \implies a = 15, b = 75,$$
$$(m, n) = (5, 1) \implies a = 75, b = 15.$$

5.

5.1. Sendo p e q dois números primos diferentes, p e q são primos entre si. Logo, pela Proposição 1.13 do Texto sobre Divisibilidade,

$$\text{mmc}(p, q) = pq.$$

Por seu turno, pelo Lema 1.11 alínea 2 do mesmo Texto, para todo $n \in \mathbb{N}$,

$$\text{mdc}(p + nq, q) = \text{mdc}(p - (-n)q, q) = \text{mdc}(p, q) = 1,$$

pelo que novamente pela Proposição 1.13,

$$\text{mmc}(p + nq, q) = (p + nq)q.$$

Estes factos conjugados permitem assim concluir que

$$\text{mmc}(p + nq, q) - \text{mmc}(p, q) = (p + nq)q - pq = nq^2.$$

5.2. Comece-se por observar que por a ser um múltiplo de p,

$$\text{mdc}(a, p) = p, \ \text{mmc}(p, a) = a.$$

Deste modo, resulta do Lema 1.11, alínea 2,

$$\text{mdc}(p + na, a) = \text{mdc}(p, a) = p,$$

o que implica, pela Proposição 1.13,

$$\text{mmc}(p+na,a) = \frac{(p+na)a}{p} = \frac{p+na}{p}\text{mmc}(p,a).$$

Como, por linearidade,

$$p \,|\, p,\ p \,|\, a \implies p \,|\, \underbrace{(p+na)}_{\in\mathbb{N}},$$

tem-se que $\frac{p+na}{p} \in \mathbb{N}$, com o que fica provado o pretendido.

6. Em termos de factorização em números primos tem-se

$$2160 = 2^4 \times 3^3 \times 5.$$

Logo:

6.1. Um número natural é um divisor de 2160 se, e só se, é da forma

$$2^\alpha \times 3^\beta \times 5^\gamma, \quad \alpha \in \{0,1,2,3,4\},\ \beta \in \{0,1,2,3\},\ \gamma \in \{0,1\}. \tag{2}$$

O número total de **divisores positivos** de 2160 é assim igual ao número de elementos da forma (α,β,γ) com $\alpha \in \{0,1,2,3,4\}$, $\beta \in \{0,1,2,3\}$ e $\gamma \in \{0,1\}$, o qual é igual a

$$\#\{0,1,2,3,4\} \times \#\{0,1,2,3\} \times \#\{0,1\} = 40.$$

Uma vez que este número inclui a unidade e o próprio 2160, temos então que o número total de **divisores próprios** positivos de 2160 é igual a $40 - 2 = 38$.

6.2. Consideremos agora todos os divisores positivos de 2160, isto é, todos os números da forma (2).

6.2.1. Como o produto de números ímpares é sempre um número ímpar, um divisor (2) de 2160 é ímpar se, e só se, $\alpha = 0$. Consequentemente, a factorização em números primos de um tal divisor é da forma

$$3^\beta \times 5^\gamma, \quad \beta \in \{0,1,2,3\},\ \gamma \in \{0,1\},$$

pelo que, como anteriormente, existem 8 divisores ímpares de 2160.

6.2.2 Os divisores positivos de 2160 que são múltiplos de 3 são todos os números da forma (2) com $\beta \neq 0$. Assim, há um total de

$$\#\{0,1,2,3,4\} \times \#\{1,2,3\} \times \#\{0,1\} = 30$$

divisores nestas condições.

6.2.3. Neste caso procuram-se todos os divisores da forma (2) tais que

$$\sqrt{2^\alpha \times 3^\beta \times 5^\gamma} = 2^{\frac{\alpha}{2}} \times 3^{\frac{\beta}{2}} \times 5^{\frac{\gamma}{2}} \in \mathbb{N}.$$

A factorização em números primos dos divisores procurados é assim da forma

$$2^\alpha \times 3^\beta, \quad \alpha \in \{0,2,4\}, \beta \in \{0,2\},$$

num total de 6 divisores.

7. Em termos de factorização de números primos tem-se

$$2160 = 2^4 \times 3^3 \times 5, \quad 525 = 3 \times 5^2 \times 7,$$

pelo que o $\mathrm{mdc}(2160, 525)$ é igual ao produto dos factores comuns, cada um elevado ao menor expoente. Por outras palavras:

$$\mathrm{mdc}(2160, 525) = 3^{\min\{3,1\}} \times 5^{\min\{1,2\}} = 3 \times 5 = 15. \tag{3}$$

Atendendo à Proposição 1.13, daqui resulta de imediato que

$$\mathrm{mmc}(2160, 525) = \frac{2160 \times 525}{\mathrm{mdc}(2160, 525)} = 2^4 \times 3^{\max\{3,1\}} \times 5^{\max\{1,2\}} \times 7 = 2^4 \times 3^3 \times 5^2 \times 7.$$

Confirmemos agora o resultado obtido em (3) pelo algoritmo de Euclides. Dividindo 2160 por 525 obtém-se $2160 = 4 \cdot 525 + 60$, pelo que

$$\mathrm{mdc}(2160, 525) = \mathrm{mdc}(525, 60).$$

De modo análogo, dividindo 525 por 60 tem-se $525 = 8 \cdot 60 + 45$, pelo que

$$\mathrm{mdc}(525, 60) = \mathrm{mdc}(60, 45).$$

Repetindo novamente este raciocínio obtém-se

$$\mathrm{mdc}(60, 45) = \mathrm{mdc}(45, 15) = 15,$$

em que na última igualdade utilizou-se o facto de $45 = 3 \times 15$ e, portanto, 15 é maior divisor comum a 15 e a 45.

8. Com vista a um absurdo, vamos supor que p não é um número primo. Assim sendo, $p = ab$. Como, por hipótese, p não é múltiplo de nenhum número menor que n tem que se ter $a, b \geq n$. Mas,

$$a, b \geq n \implies p = ab \geq n^2,$$

o que é um absurdo, pois, por hipótese, $p < n^2$. Como o absurdo resultou da hipótese de p não ser um número primo, conclui-se então que p é primo.

9.

9.1. Para qualquer $k = 1, 2, \ldots, p-1$ tem-se

$$p! = \binom{p}{k}(p-k)!k!$$

Como $p! = p(p-1)!$, $(p-1)! \in \mathbb{N}$, resulta então que $p \,|\, p!$ e, portanto,

$$p \,|\, \binom{p}{k}(p-k)!k! \tag{4}$$

O resto do exercício resume-se a provar que

$$p \not| (p-k)!k!, \quad k = 1, 2, \ldots, p-1. \tag{5}$$

Com efeito, provado (5), resulta do facto de p ser primo e do Lema 1.11 alínea 1 do texto sobre Divisibilidade que $\text{mdc}(p,(p-k)!k!)=1$ e, portanto, por (4) e pela Proposição 1.9 do mesmo texto, $p \mid \binom{p}{k}$, $k=1,2,\ldots,p-1$.

Para provar (5) comece-se por notar que

$$k \equiv -(p-k) \,(\text{mod}\, p)$$

ou, mais geralmente,

$$k-i \equiv -(p-k+i) \,(\text{mod}\, p), \quad i=0,1,\ldots,k-1.$$

Assim sendo,

$$\begin{aligned} k!(p-k)! &\equiv (-1)^k (p-k) \underbrace{(p-k+1)\ldots(p-2)(p-1)(p-k)!}_{=(p-1)(p-2)\ldots(p-k+1)(p-k)!=(p-1)!} \,(\text{mod}\, p) \\ &\equiv (-1)^k (p-k)(p-1)! \,(\text{mod}\, p), \end{aligned}$$

onde, pelo Teorema 1.34 (Wilson),

$$(p-1)! \equiv -1 \,(\text{mod}\, p)$$

por p ser primo. Consequentemente,

$$k!(p-k)! \equiv (-1)^{k+1}(p-k) \,(\text{mod}\, p),$$

em que por $k=1,2,\ldots,p-1$ (ou seja, por $k \neq 0$, $k \neq p$), $(p-k) \not\equiv 0 \,(\text{mod}\, p)$. Logo, $k!(p-k)! \not\equiv 0 \,(\text{mod}\, p)$, o que equivale a (5).

9.2. Comece-se por observar que $(p-1)!$ é um múltiplo comum de $1,2,\ldots,p-1$. Logo, por definição de mínimo múltiplo comum,

$$\text{mmc}(1,2,\ldots,p-1) \mid (p-1)! \tag{6}$$

Daqui resulta que p não divide $\text{mmc}(1,2,\ldots,p-1)$. Com efeito, se p fosse um divisor de $\text{mmc}(1,2,\ldots,p-1)$, então, por transitividade, resultaria de (6) que p dividiria $(p-1)!$, o que é impossível, como provado em (5) da alínea anterior. Logo,

$$p \not| \,\text{mmc}(1,2,\ldots,p-1).$$

Este resultado prova a afirmação feita no início da demonstração do Teorema 1.35 (Teorema de Wolstenholme).

9.3. Provemos o resultado pretendido por recurso ao método de indução matemática. Assim:

Case Base: $\mathbf{n=0}$. Este caso é imediato, pois qualquer número não nulo divide o 0.

Hipótese de indução: Fixado um $n \in \mathbb{N}$, **qualquer**, suponhamos que

$$p \,|\, (n^p - n).$$

Tese de indução:

$$p \,|\, ((n+1)^p - (n+1)).$$

Passo de indução: Pelo Binómio de Newton tem-se

$$\begin{aligned}(n+1)^p - (n+1) &= \sum_{k=0}^{p} \binom{p}{k} n^{p-k} - (n+1) \\ &= n^p + \binom{p}{1} n^{p-1} + \ldots + \binom{p}{p-1} n + 1 - (n+1) \\ &= (n^p - n) + \binom{p}{1} n^{p-1} + \ldots + \binom{p}{p-1} n,\end{aligned}$$

em que, pela hipótese de indução, $n^p - n$ é divisível por p, enquanto que os restantes termos são divisíveis por p pela alínea 9.1. Deste modo prova-se que p é divisor de $(n+1)^p - (n+1)$.

Conclusão: Pelo método de indução matemática, fica assim provado que

$$p \,|\, (n^p - n), \quad \forall\, n \in \mathbb{N}.$$

10. A resolução destes dois exercícios segue as linhas da demonstração do critério de divisibilidade por 7. Tal como nesse caso, também agora 13 e 37 são números primos e, por conseguinte, todos os elementos de $\mathbb{Z}_{13} \setminus \{\bar{0}\}$ e de $\mathbb{Z}_{37} \setminus \{\bar{0}\}$ são invertíveis.

10.1. Dado

$$N = \sum_{k=0}^{n} a_k 10^k,$$

consideremos novamente

$$N - a_0 = 10 \sum_{k=1}^{n} a_k 10^{k-1}.$$

Como

$$10 \cdot 4 \equiv 1 \,(\mathrm{mod}\, 13),$$

tem-se então

$$4(N - a_0) = 40 \sum_{k=1}^{n} a_k 10^{k-1} \equiv \sum_{k=1}^{n} a_k 10^{k-1} \,(\mathrm{mod}\, 13),$$

o que conduz, por subtracção de $9a_0$ a "ambos os membros", a

$$4N \equiv \sum_{k=1}^{n} a_k 10^{k-1} - 9a_0 \,(\mathrm{mod}\, 13).$$

Desta forma, tem-se que

$$\sum_{k=1}^{n} a_k 10^{k-1} - 9a_0 = (a_n a_{n-1} \dots a_1)_{10} - 9a_0$$

é divisível por 13 se, e só se, $4N$ é divisível por 13, o que acontece se, e só se, N é divisível por 13 (cf. Proposição 1.9).

10.2. Novamente partindo de

$$N - a_0 = 10 \sum_{k=1}^{n} a_k 10^{k-1}, \; N := \sum_{k=0}^{n} a_k 10^k,$$

resulta de $26 \cdot 10 \equiv 1 \pmod{37}$,

$$26(N - a_0) = 260 \sum_{k=1}^{n} a_k 10^{k-1} \equiv \sum_{k=1}^{n} a_k 10^{k-1} \pmod{37},$$

pelo que

$$26N \equiv 26(N - a_0) - 11a_0 \equiv \sum_{k=1}^{n} a_k 10^{k-1} - 11a_0 \pmod{37}.$$

Desta maneira conclui-se que

$$\sum_{k=1}^{n} a_k 10^{k-1} - 11a_0 = (a_n a_{n-1} \dots a_1)_{10} - 11a_0$$

é divisível por 37 se, e só se, $26N$ é divisível por 37, o que acontece se, e só se, N é divisível por 37 (cf. Proposição 1.9).

11. Comece-se por observar que $71392 = 4 \times 17848$. Assim, de acordo com a demonstração do critério de divisibilidade por 13 (Exercício 10.1), tem-se que

$$71392 = 4 \times 17848 \equiv \underbrace{1784 - 9 \times 8}_{=1712} \pmod{13}.$$

Do mesmo modo,

$$1712 = 4 \times 428 \equiv \underbrace{42 - 9 \times 8}_{=-30} \pmod{13}.$$

Ou seja e por transitividade,

$$71392 \equiv -30 \pmod{13},$$

pelo que o resto da divisão de 71392 por 13 é igual ao resto da divisão de -30 por 13, ou seja, 9 (pela divisão euclidiana, $-30 = 13 \times (-3) + 9$).