Lista 3 com respostas

MAT0120 — 1° SEMESTRE DE 2020

Equações Diofantinas

Exercício 1.
Resolva as seguintes equações diofantinas:

a) $3x + 5y = 47$,

b) $47x + 29y = 99$.

Solução 1.

a) Como $\text{mdc}(3, 5) = 1$ e $1 \mid 47$, então a equação tem solução.

$$3 \cdot 2 + 5 \cdot (-1) = 1$$

$$3 \cdot 94 + 5 \cdot (-47) = 47.$$

Assim, $x_0 = 94$ e $y_0 = -47$ é uma solução particular da equação diofantina, enquanto todas as soluções são do tipo $S = \{(94 + 5t, -47 - 3t) : t \in \mathbb{Z}\}$.

b) Como $\text{mdc}\,(47, 29) = 1$ e $1 \mid 99$, então a equação tem solução.

$$47 \cdot (-1) + 29 \cdot 2 = 11$$

$$47 \cdot (-9) + 29 \cdot 18 = 99.$$

Assim, $x_0 = -9$ e $y_0 = 18$ é uma solução particular da equação diofantina, enquanto todas as soluções são do tipo $S = \{(-9 + 29t, 18 - 47t) : t \in \mathbb{Z}\}$.

Exercício 2.
Determine todas as soluções inteiras das equações abaixo que verificam $x \geqslant 0$, e $y \geqslant 0$.

a) $54x + 21y = 906$,

b) $30x + 17y = 300$.

Solução 2.

a) Como $\text{mdc}\,(54, 21) = 3$ e $3 \mid 906$, então a equação tem solução.

$$54x + 21y = 906$$

$$18x + 7y = 302$$

$$18 \cdot 2 + 7 \cdot (-5) = 1$$

$$18 \cdot 604 + 7 \cdot (-1510) = 302$$

Assim, $x_0 = 604$ e $y_0 = -1510$ é uma solução particular da equação diofantina, enquanto todas as soluções são do tipo $S = \{(604 + 7t, -1510 - 18t) : t \in \mathbb{Z}\}$. Como $x \geqslant 0$ e $y \geqslant 0$, temos:

$$\begin{cases} 604 + 7t \geqslant 0 \\ -1510 - 18t \geqslant 0 \end{cases} \overset{t\in\mathbb{Z}}{\Longrightarrow} t \in \{-86, -85, -84\}$$

Portanto, as soluções pertencem ao conjunto $S = \{(2, 38), (9, 20), (16, 2)\}$.

b) Como mdc $(30, 17) = 1$ e $1 \mid 300$, então a equação tem solução.

$$30 \cdot (-1) + 17 \cdot 2 = 4$$

$$30 \cdot (-75) + 17 \cdot 150 = 300.$$

Assim, $x_0 = -75$ e $y_0 = 150$ é uma solução particular da equação diofantina, enquanto todas as soluções são do tipo $S = \{(-75 + 17t, 150 - 30t) : t \in \mathbb{Z}\}$. Como $x \geqslant 0$ e $y \geqslant 0$, temos:

$$\begin{cases} -75 + 17t \geqslant 0 \\ 150 - 30t \geqslant 0 \end{cases} \overset{t\in\mathbb{Z}}{\Longrightarrow} t = 5$$

Portanto, a solução é $S = \{(10, 0)\}$.

Exercício 3.

Seja p um primo. Prove que a equação $x^4 + 4y^4 = p$ tem solução inteira se e só se $p = 5$. Nesse caso, determine suas soluções.

Solução 3.

$$\begin{aligned} p &= x^4 + 4y^4 \\ &= \left(x^2 + 2y^2\right)^2 - 4x^2y^2 \\ &= \left(x^2 + 2xy + 2y^2\right)\left(x^2 - 2xy + 2y^2\right) \\ &= \left((x+y)^2 + y^2\right)\left((x-y)^2 + y^2\right) \end{aligned}$$

Note que os dois fatores são não negativos. Como p é primo, um deles deve ser igual a 1. Assim, temos as seguintes possibilidades:

$$\begin{cases} \left((x+y)^2 = 1 \wedge y^2 = 0\right) \vee \left((x+y)^2 = 0 \wedge y^2 = 1\right) \\ \qquad\qquad\qquad\qquad \vee \\ \left((x-y)^2 = 1 \wedge y^2 = 0\right) \vee \left((x-y)^2 = 0 \wedge y^2 = 1\right) \end{cases} \Rightarrow$$

$$\begin{cases} (x = 1 \wedge y = 0) \vee (x = -1 \wedge y = 0) \vee (x = -1 \wedge y = 1) \vee (x = 1 \wedge y = -1) \\ \qquad\qquad\qquad\qquad \vee \\ (x = 1 \wedge y = 1) \vee (x = -1 \wedge y = -1) \end{cases}$$

Para $x = \pm 1$ e $y = 0$, $p = 1$ não é primo, e para $x = \pm 1$ e $y = \pm 1$, $p = 5$.

Exercício 4.
Determine todos os múltiplos positivos de 11 e 9 cuja soma seja 270.

Solução 4.
O exercício busca as soluções naturais da equação diofantina

$$11x + 9y = 270$$

Como mdc $(11, 9) = 1$ e $1 \mid 270$, a equação tem solução.

$$11 \cdot 1 + 9 \cdot (-1) = 2$$

$$11 \cdot 135 + 9\,(-135) = 270$$

Assim, $x_0 = 135$ e $y_0 = -135$ é uma solução particular da equação diofantina, enquanto todas as soluções são do tipo $S = \{(135 + 9t, -135 - 11t) : t \in \mathbb{Z}\}$. Como $x \geqslant 0$ e $y \geqslant 0$, temos:

$$\begin{cases} 135 + 9t > 0 \\ -135 - 11t > 0 \end{cases} \overset{t\in\mathbb{Z}}{\Longrightarrow} t = -13 \vee t = -14$$

Portanto, as soluções são $11 \cdot 18 = 198$ e $9 \cdot 8 = 72$ ou $11 \cdot 9 = 99$ e $9 \cdot 19 = 171$.

Exercício 5.
Determine todos os inteiros positivos menores de que 1000 que têm restos 9 e 15 quando divididos respectivamente por 37 e 52.

Solução 5.
Queremos encontrar $n \in \mathbb{N}; n < 1000$, tal que:

$$\begin{cases} n = 37x + 9 \\ n = 52y + 15 \end{cases} \Rightarrow 37x - 52y = 6; x, y \in \mathbb{N}$$

Como mdc $(37, 52) = 1$ e $1 \mid 6$, a equação diofantina tem solução.

$$37 \cdot (-7) - 52 \cdot (-5) = 1$$

$$37 \cdot (-42) - 52 \cdot (-30) = 6$$

Assim, $x_0 = -42$ e $y_0 = -30$ é uma solução particular da equação diofantina, enquanto todas as soluções são do tipo $S = \{(-42 - 52t, -30 - 37t) : t \in \mathbb{Z}\}$. Como $1000 > n \geqslant 0$, temos:

$$\begin{cases} 1000 > 37x + 9 > 0 \\ 1000 > 52y + 15 > 0 \end{cases} \Rightarrow \begin{cases} \frac{991}{37} > x > -\frac{9}{37} \\ \frac{985}{52} > y > -\frac{15}{52} \end{cases} \Rightarrow \begin{cases} \frac{991}{37} > -42 - 52t > -\frac{9}{37} \\ \frac{985}{52} > -30 - 37t > -\frac{15}{52} \end{cases} \Rightarrow$$

$$\begin{cases} \frac{2545}{37} > -52t > \frac{1545}{37} \\ \frac{2545}{52} > -37t > \frac{1545}{52} \end{cases} \Rightarrow \begin{cases} -\frac{2545}{1924} < t < -\frac{1545}{1924} \\ -\frac{2545}{1924} < t < -\frac{1545}{1924} \end{cases} \overset{t\in\mathbb{Z}}{\Longrightarrow} t = -1.$$

Assim, $x = 10$ e $y = 7$. Portanto, o único número é $n = 37 \cdot 10 + 9 = 379$.

Exercício 6.
Somando-se um certo múltiplo $6x$ de 6 com certo múltiplo $9y$ de 9, obtém-se 126. Trocando x por y e y por x, a nova soma é 114. Determine x e y.

Solução 6.
$$\begin{cases} 6x + 9y = 126 \\ 9x + 6y = 114 \end{cases} \Rightarrow \begin{cases} 2x + 3y = 42 \\ 3x + 2y = 38 \end{cases} \Rightarrow \begin{cases} 4x + 6y = 84 \\ 9x + 6y = 114 \end{cases} \Rightarrow \begin{cases} 5x = 30 \\ 9x + 6y = 114 \end{cases} \Rightarrow \begin{cases} x = 6 \\ y = 10 \end{cases}$$

Exercício 7.
Se x e y são inteiros tais que $2x + 3y$ é múltiplo de 17, prove então que $9x + 5y$ é também múltiplo de 17.

Solução 7.
Vamos resolver a equação diofantina

$$2x + 3y = 17k; k \in \mathbb{Z}$$

Como mdc $(2, 3) = 1$ e $1 \mid 17k$, então ela possui solução.

$$2 \cdot (-1) + 3 \cdot 1 = 1$$

$$2 \cdot (-17k) + 3 \cdot 17k = 17k$$

Assim, as soluções são $x = -17k + 3t$ e $y = 17k - 2t$, para $t \in \mathbb{Z}$.

Logo:

$$\begin{aligned} 9x + 5y &= 9 \cdot (-17k + 3t) + 5 \cdot (17k - 2t) \\ &= -4 \cdot 17k + 17t \\ &= 17\,(-4k + t) \end{aligned}$$

Portanto $17 \mid 9x + 5y$.

Exercício 8.
Certo senhor, ao descontar um cheque, recebeu sem notar o número de reais trocado pelo número de centavos e vice-versa. Em seguida, gastou 68 centavos e observou, surpreso, que tinha o dobro da quantia original do cheque. Determine o menor valor possível para o cheque.

Solução 8.
Seja a quantia certa de x reais e y centavos. Assim, o senhor deveria receber $100x + y$ centavos, mas recebeu $100y + x$ centavos. Logo, $100y + x - 68 = 2\,(100x + y) \Rightarrow -199x + 98y = 68$.

Como mdc $(98, 199) = 1$ e $1 \mid 68$, a equação diofantina tem solução. Pelo algoritmo de Euclides, temos:

$$1 = -199 \cdot (-33) + 98 \cdot (-67)$$

$$68 = -199 \cdot (-2244) + 98 \cdot (-4556)$$

Assim, $x_0 = -2244$ e $y_0 = -4556$ é uma solução particular da equação diofantina, enquanto todas as soluções são do tipo $S = \{(-2244 + 98t, -4556 + 199t) : t \in \mathbb{Z}\}$.

Como $x > 0$ e $y > 0$, temos:

$$\begin{cases} -2244 + 98t > 0 \\ -4556 + 199t > 0 \end{cases} \Rightarrow t \geqslant 23$$

Assim, temos $t = 23 \Rightarrow x = 10 \wedge y = 21$, totalizando R$\$10,21$.

Exercício 9.
Um pescador tenta pescar um cardume jogando diversas redes na água. Se cair exatamente um peixe em cada rede, salvam-se ainda n peixes. Se caírem n peixes em cada rede, sobram n redes vazias. Quantas são as redes? Quantos são os peixes?

Solução 9.
Sejam t e r o número total de peixes e de redes, respectivamente. Assim:

$$\begin{cases} t = 1 \cdot r + n \\ t = n\,(r - n) \end{cases} \Rightarrow \begin{cases} t = r + n \\ r + n = nr - n^2 \end{cases} \Rightarrow r = \frac{n^2 + n}{n - 1} = n + 2 + \frac{2}{n - 1}$$

Como $r, n \in \mathbb{N}$, temos que $n - 1 \mid 2 \Leftrightarrow n = 2 \vee n = 3$.

Se $n = 2$, temos $r = 6$ redes e $t = 8$ peixes. Se $n = 3$, temos $r = 6$ redes e $t = 9$ peixes.

Exercício 10.
Uma pessoa tem R$ 13,60 para gastar em cervejas e refrigerantes. Se cada cerveja custa R$ 1,50 e cada refrigerante custa R$ 0,70 quantas cervejas e quantos refrigerantes ela poderá comprar?

Solução 10.
Sejam $C, R \in \mathbb{N}$ os números de cervejas e refrigerantes em centavos. Assim, temos:

$$150C + 70R = 1360$$

$$15C + 7R = 136$$

Como mdc $(15, 7) = 1$ e $1 \mid 136$, a equação diofantina tem solução.

$$15 \cdot 1 + 7 \cdot (-2) = 1$$

$$15 \cdot 136 + 7 \cdot (-272) = 136$$

Assim, $C_0 = 136$ e $R_0 = -27$ é uma solução particular da equação diofantina, enquanto todas as soluções são do tipo $S = \{(136 + 7t, -272 - 15t) : t \in \mathbb{Z}\}$.

Como $C > 0$ e $R > 0$, temos:

$$\begin{cases} 136 + 7t > 0 \\ -272 - 15t > 0 \end{cases} \overset{t \in \mathbb{Z}}{\Longrightarrow} t = -19.$$

Portanto $C = 3$ e $R = 13$.

Exercício 11.
Uma certa tinta pode ser comprada em galões de $18\mathrm{L}$ ou em latas de $3\mathrm{L}$. Precisa-se de $250\mathrm{L}$ dessa tinta. De quantas maneiras se pode comprar latas e galões para que a quantidade de sobra seja mínima?

Solução 11.
Sejam $\mathsf{G}, \mathsf{L} \in \mathbb{N}$ os números de galões e latas. Queremos resolver a seguinte equação diofantina:

$$18\mathsf{G} + 3\mathsf{L} = 250$$

Como $\text{mdc}\,(18, 3) = 3$ e $3 \nmid 250$, a equação diofantina não tem solução. Assim, vamos fazer uma combinação de galões e latas para conseguirmos 252 litros, que é o menor múltiplo de 3 maior que 252.

$$18\mathsf{G} + 3\mathsf{L} = 252$$

$$6\mathsf{G} + 1\mathsf{L} = 84$$

Como $\text{mdc}\,(6, 1) = 1$ e $1 \mid 84$, a equação diofantina tem solução. Assim:

$$6 \cdot 1 + 1 \cdot (-5) = 1$$

$$6 \cdot 84 + 1 \cdot (-420) = 84.$$

Assim, $\mathsf{G}_0 = 84$ e $\mathsf{L}_0 = -420$ é uma solução particular da equação diofantina, enquanto todas as soluções são do tipo $\mathsf{S} = \{(84 + 1\mathsf{t}, -420 - 6\mathsf{t}) : \mathsf{t} \in \mathbb{Z}\}$.

Como $\mathsf{G} \geqslant 0$ e $\mathsf{R} \geqslant 0$, temos:

$$\begin{cases} 84 + 1\mathsf{t} \geqslant 0 \\ -420 - 6\mathsf{t} \geqslant 0 \end{cases} \overset{\mathsf{t} \in \mathbb{Z}}{\Longrightarrow} \mathsf{t} \in \{-84, -83, \cdots, -70\}$$

Portanto, temos 15 soluções diferentes para o par $(\mathsf{G}, \mathsf{L}) : (0, 84), (1, 78), \cdots, (14, 0)$.

Exercício 12.
Um hospital deseja adquirir medicamentos A e B de modo a distribuí-los entre alguns pacientes. Cada paciente receberá 20 vidros de cada medicamento devendo ainda sobrar 84 vidros de cada medicamento. Sabendo que A é vendido em caixas de 132 vidros e B, em caixas de 242 vidros, determine:

a) o número mínimo de caixas de cada medicamento que o hospital deve comprar;

b) o número de pacientes que receberão os medicamentos.

Solução 12.
Sejam $\mathsf{A}, \mathsf{B}, \mathsf{P} \in \mathbb{N}$ o número de caixas do medicamento A, do medicamento B e de pacientes, respectivamente. Assim:

$$\begin{cases} 132\mathsf{A} = 20\mathsf{P} + 84 \\ 242\mathsf{B} = 20\mathsf{P} + 84 \end{cases} \Rightarrow \begin{cases} 242\mathsf{B} = 132\mathsf{A} \\ \mathsf{P} = \frac{132\mathsf{A} - 84}{20} \end{cases} \Rightarrow \begin{cases} 11\mathsf{B} = 6\mathsf{A} \\ \mathsf{P} = \frac{33\mathsf{A} - 21}{5} \end{cases} \Rightarrow \begin{cases} \mathsf{B} = \frac{6}{11}\mathsf{A} \\ \mathsf{P} = \frac{3(11\mathsf{A} - 7)}{5} \end{cases} .$$

a) Para que A , B e P sejam inteiros. é necessário que $11 \mid A$ e $5 \mid 11A - 7$. Logo, o menor valor de A para que isso aconteça é $A = 22$ e, portanto, $B = 12$.

b) $P = \dfrac{132 \cdot 22 - 84}{20} = 141$.

Números primos e Teorema Fundamental da Aritmética

Exercício 13.
Encontre todos os inteiros positivos a tais que

$$\begin{cases} \text{mmc}(120, a) &= 360 \\ \text{mdc}(450, a) &= 90 \end{cases}$$

Solução 13.

$$\left.\begin{array}{l} 120 = 2^3 \cdot 3^1 \cdot 5^1 \\ 360 = 2^3 \cdot 3^2 \cdot 5^1 \end{array}\right\} \Rightarrow \text{mmc}\,(120, a) = 360 \Rightarrow a = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3};\ \text{com} \begin{array}{r} \alpha_1 \in \{0,1,2,3\} \\ \alpha_2 \in \{0,1,2\} \\ \alpha_3 \in \{0,1\} \end{array}.$$

$$\left.\begin{array}{l} 450 = 2^1 \cdot 3^2 \cdot 5^2 \\ 90 = 2^1 \cdot 3^2 \cdot 5^1 \end{array}\right\} \Rightarrow \text{mdc}\,(450, a) = 90 \Rightarrow a = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3} \cdots;\ \text{com} \begin{array}{r} \alpha_1 \in \{1,2,\cdots\} \\ \alpha_2 \in \{2,3,\cdots\} \\ \alpha_3 = 1 \end{array}.$$

Logo, $\alpha_1 \in \{1,2,3\}$, $\alpha_2 = 2$ e $\alpha_3 = 1$. Assim, $a \in \{90, 180, 360\}$.

Exercício 14.
Resolva em $\mathbb{Z}$ o sistema abaixo

$$\begin{cases} \text{mmc}(x, y) &= 420 \\ \text{mdc}(x, y) &= 20 \end{cases}$$

Solução 14.
Sejam $x = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3} \cdot 7^{\alpha_4} \cdots$ e $y = 2^{\beta_1} \cdot 3^{\beta_2} \cdot 5^{\beta_3} \cdot 7^{\beta_4} \cdots$

$$\begin{array}{l} \text{mmc}\,(x, y) = 420 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1 \\ \text{mdc}\,(x, y) = 20 = 2^2 \cdot 5^1 \end{array}$$

Logo:

$$\begin{array}{l} \alpha_1 = \beta_1 = 2 \\ \alpha_2 + \beta_2 = 1 \\ \alpha_3 = \beta_3 = 2 \\ \alpha_4 + \beta_4 = 1 \end{array}$$

Temos duas escolhas para fazer no expoente do 3 e no expoente do 7. Todas as combinações possíveis são:

$$(x, y) \in \{(\pm 420, \pm 20), (\pm 60, \pm 140), (\pm 140, \pm 60), (\pm 20, \pm 420)\}.$$

Exercício 15.
Seja n um inteiro positivo. Mostre que se n divide $(n-1)!+1$, então n é primo. (*Dica:* Tome um divisor primo p de n e mostre que $p \geqslant n$.)

Solução 15.
Suponha, por absurdo, que n seja composto. Logo, $n = p \cdot k$, com p e k inteiros, e p primo.

Sabemos que $p \leqslant n - 1$, assim, na expansão $(n-1)! = (n-1) \cdot (n-2) \cdots 2 \cdot 1$, certamente teremos um fator p. Portanto, $p \mid (n-1)!$.

Mas se p divide n e p divide $(n-1)!$, então p divide 1, o que é absurdo.

Portanto, n é primo.

Exercício 16.
Seja $a, b \in \mathbb{Z}$ tais que $\text{mdc}(a, b) = p$, um inteiro primo. O que se pode dizer sobre $\text{mdc}(a^2, b)$ e $\text{mdc}(a^2, b^2)$?

Solução 16.
Sejam $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k} \cdots p_n^{\alpha_n}$ e $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_k^{\beta_k} \cdots p_m^{\alpha_m}$, sendo p_i os números primos e α_i e β_i números naturais, incluindo o zero.

Assim:

$$\begin{aligned} \text{mdc}\,(a, b) &= p_1^{\min\{\alpha_1, \beta_1\}} \cdot p_2^{\min\{\alpha_2, \beta_2\}} \cdots \\ &= p_k^{\min\{\alpha_k, \beta_k\}} \\ &= p \end{aligned}$$

Nesse caso, ou $\alpha_k = 1$ ou $\beta_k = 1$.

Então, temos:

$$\begin{aligned} \text{mdc}\left(a^2, b\right) &= p_1^{\min\{2\alpha_1, \beta_1\}} \cdot p_2^{\min\{2\alpha_2, \beta_2\}} \cdots \\ &= p_k^{\min\{2\alpha_k, \beta_k\}}. \end{aligned}$$

Temos dois casos:

- $a_k = 1$ e $\beta_k = 2 \Rightarrow \text{mdc}\left(a^2, b\right) = p_k^{\min\{2,2\}} = p_k^2 = p^2$
- $\beta_k = 1 \Rightarrow \text{mdc}\left(a^2, b\right) = p_k^{\min\{2\alpha_k, 1\}} = p_k^1 = p$

Assim, $\text{mdc}\left(a^2, b\right)$ ou é p ou é p^2, dependendo dos números a e b.

$$\begin{aligned} \text{mdc}\left(a^2, b^2\right) &= p_1^{\min\{2\alpha_1, 2\beta_1\}} \cdot p_2^{\min\{2\alpha_2, 2\beta_2\}} \cdots \\ &= p_1^{2\min\{\alpha_1, \beta_1\}} \cdot p_2^{2\min\{\alpha_2, \beta_2\}} \cdots \\ &= p_k^{2\min\{\alpha_k, \beta_k\}} \\ &= p_k^{2 \cdot 1} \\ &= p^2. \end{aligned}$$

Exercício 17.
Mostrar que três inteiros positivos ímpares consecutivos não podem ser todos primos, com exceção de 3,5, e 7.

Solução 17.
Sejam $n, n+2$ e $n+4$ os três primos ímpares consecutivos. Pelo algoritmo da divisão, $n = 3k+r; k \in \mathbb{Z}$ e $r \in \{0, 1, 2\}$.

- se $n = 3k$, então n é múltiplo de 3. O único primo múltiplo de 3 é $n = 3$, logo $n + 2 = 5$ e $n + 4 = 7$;
- se $n = 3k+1$, então $n+2 = 3k+3 = 3k'$. O único primo múltiplo de 3 é $n+2 = 3$, logo $n = 1$, o que não convém;
- se $n = 3k + 2$, então $n + 4 = 3k + 3 = 3k'$. O único primo múltiplo de 3 é $n + 4 = 3$, logo $n = -1$, o que não convém.

Exercício 18.
Sejam p, q primos tais que $p \geqslant q \geqslant 5$. Provar que $24|p^2 - q^2$.

Solução 18.
Como $p, q \geqslant 5$, então p e q são ímpares. Assim, pelo algoritmo da divisão, p e q são do tipo $2k + 1$. Sejam $p = 2a + 1$ e $q = 2b + 1$, com $a, b \in \mathbb{Z}$. Logo:

$$p^2 - q^2 = (p + q)(p - q) = (2a + 2b + 2)(2a - 2b) = 4(a + b + 1)(a - b).$$

Como $(a + b + 1)$ e $(a - b)$ possuem paridades distintas, um destes termos é par. Assim, $p^2 - q^2$ é múltiplo de 8.

Como $p, q \geqslant 5$, entãop e q são maiores que 5, pelo algoritmo da divisão, eles são da forma $3k + 1$ ou $3k + 2$, caso contrário eles seriam múltiplos de 3. Aqui, temos 3 opções: ou ambos são do tipo $3k + 1$, ou ambos são do tipo $3k + 2$ ou cada um é de um tipo. Vamos analisar estas 3 opções:

- $p = 3k + 1 \wedge q = 3t + 1 \Rightarrow p^2 - q^2 = (3k + 3t + 2)(3k - 3t) = 3(3k + 3t + 2)(k - t)$;
- $p = 3k+2 \wedge q = 3t+1 \Rightarrow p^2-q^2 = (3k + 3t + 3)(3k - 3t + 1) = 3(k + t + 1)(3k - 3t + 1)$;
- $p = 3k + 2 \wedge q = 3t + 2 \Rightarrow p^2 - q^2 = (3k + 3t + 4)(3k - 3t) = 3(3k + 3t + 4)(k - t)$.

Em todos os casos, $p^2 - q^2$ é múltiplo de 3 .

Como $8 \mid p^2 - q^2$ e $3 \mid p^2 - q^2$, então mmc $(3, 8) = 24 \mid p^2 - q^2$.

Exercício 19.
Seja n um inteiro positivo. Provar que

a) Se $2^n - 1$ é primo então n é primo;

b) $n^4 + 4$ é composto, para todo $n > 1$;

c) todo inteiro positivo da forma $3n + 2$ tem um fator primo dessa forma;

d) Se $n^3 - 1$ é primo, então $n = 2$;

e) Se n é primo e $3n + 1$ é um quadrado, então $n = 5$.

Solução 19.

a) Vamos provas pela contrapositiva: se n é composto, então $2^n - 1$ é composto.

Seja $n = p \cdot k$, sendo $2 < p < k < n$ e $p, k \in \mathbb{Z}$. Logo, $2^n - 1 = 2^{p \cdot k} - 1$. Independente da paridade de $p \cdot k$, podemos fatorar a expressão:

$$2^{p \cdot k} - 1 = (2^p)^k - 1 = (2^p - 1)\left((2^p)^{k-1} + (2^p)^{k-2} + \cdots + 1\right).$$

Como $p > 2$, nenhum dos fatores acima é igual a 1. Logo, $2^{p \cdot k}$ é composto.

b)

$$n^4 + 4 = n^4 + 4n^2 + 4 - 4n^2 = \left(n^2 + 2\right)^2 - (2n)^2 = \left(n^2 + 2n + 2\right)\left(n^2 - 2n + 2\right).$$

Se n for primo, então um dos fatores acima é igual a 1. Logo:

$$\begin{cases} n^2 + 2n + 2 = 1 \\ \quad \vee \\ n^2 - 2n + 2 = 1 \end{cases} \Rightarrow n = -1 \vee n = 1.$$

No entanto, $n > 1$, portando $n^4 + 4$ é composto.

c) Suponha por absurdo que o número $3n+2$ não tenha fatores do tipo $3k+2$. Assim, ele é composto por fatores $3k$ ou $3k + 1$ apenas. No entanto, multiplicando esses dois tipos de fatores, nunca teremos um número da forma $3n + 2$:

- $3k \cdot 3k' = 3k''$;
- $3k \cdot (3k' + 1) = 3k''$;
- $(3k + 1) \cdot (3k' + 1) = 9 \cdot k \cdot k' + 3k + 3k' + 1 = 3k'' + 1$.

Ou seja, é necessário que haja ao menos um fator do tipo $3k + 2$ em um número do tipo $3n + 2$.

d)

$$n^3 - 1 = (n - 1)\left(n^2 + n + 1\right).$$

Se $n^3 - 1$ é primo, então um dos fatores acima é igual a 1 . Assim:

$$\begin{cases} n - 1 = 1 \\ \quad \vee \\ n^2 + n + 1 = 1 \end{cases} \Rightarrow n = 2 \vee n = 0 \vee n = -1.$$

Como n é positivo, temos para $n = 2$, temos $n^3 - 1 = 7$, que é primo.

e) Seja $m \in \mathbb{Z}$, tal que $3n + 1 = m^2$. Pelo algoritmo da divisão, $m = 3k + r; k \in \mathbb{Z}$ e $r \in \{0, 1, 2\}$.

- $r = 0 \Rightarrow 3n + 1 = 3 \cdot \left(3k^2\right) \Rightarrow \nexists n \in \mathbb{Z}$;

- $r = 1 \Rightarrow 3n + 1 = 3\left(3k^2 + 2k\right) + 1 \Rightarrow n = 3k^2 + 2k = k\,(3k + 2)$. Como n é primo, um dos fatores anteriores deve ser 1, logo $k = 1$ e $n = 1 \cdot (3 \cdot 1 + 2) = 5$;
- $r = 2 \Rightarrow 3n + 1 = 3\left(3k^2 + 4k + 1\right) + 1 \Rightarrow n = 3k^2 + 4k + 1 = (k + 1)\,(3k + 1)$. Como n é primo, um dos fatores anteriores deve ser 1, logo $k = 0$ ou $k = -2$. Mas $k = 0 \Rightarrow n = 1$ e $k = -2 \Rightarrow n = 5$.

Portanto, a única opção válida é $n = 5$.

Exercício 20.

a) Determinar a maior potência de 14 que divide $100!$;

b) Determinar todos os primos que dividem $50!$.

Solução 20.

a) Um número para ser divisível por 14 deve ser divisível por 2 e por 7 . Em $100! = 100 \cdot 99 \cdots 2 \cdot 1$ há claramente mais números que possuem 2 como fator na decomposição prima do que números que possuem 7 como fator na decomposição prima.

Os números que possuem 7 como fator pertencem ao conjunto $\{7, 14, 21, \cdots, 49, \cdots, 98\}$. São 14 números, cada um com um fator 7, com exceção do 49 que possui 2 fatores 7. Logo, na decomposição de $100!$, o 7 fica elevado a 15^{a} potência, portanto, a maior potência de 14 que divide $100!$ é 19.

b) Os primos que pertencem a decomposição de $50! = 50 \cdot 49 \cdots 2 \cdot 1$ são os primos positivos menores ou iguais a 50. Pelo crivo de Eratóstenes, os primos menores ou iguais a 50 pertencem ao conjunto $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47\}$.

Exercício 21.

Mostre que existem infinitos primos da forma $3n + 2$, com $n \in \mathbb{Z}$.

Solução 21.

Suponha que haja finitos números primos da forma $3k+2$, a saber, $p_1 = 3q_1+2$, $p_2 = 3q_2+2, \cdots, p_k = 3q_k + 2$, com $p_1 < p_2 < \cdots < p_k$ e seja $S = \{p_1, p_2, \cdots, p_k\}$.

Agora, tome $x = p_1 \cdot p_2 \cdots p_k$, que é da forma $3k + 1$ ou $3k + 2$. Seja também $x^2 = (p_1 \cdot_2 \cdots p_k)^2$, que é certamente da forma $3k + 1$. Por fim, seja $x^2 + 1 \in \mathbb{Z}$.

Sabemos que $x^2 + 1$ é da forma $3k + 2$, agora vamos provar que $x^2 + 1$ é primo. Supondo que seja composto, existe $p_i \in S$ que divide $x^2 + 1$, o que é absurdo, porque $p_i \mid x$, logo $p_i \mid 1$.

Como $x^2 + 1$ é primo e da forma $3k + 2$ então $x^2 + 1 \in S$. No entanto, $p_k < x < x^2 + 1$, o que é absurdo, pois p_k era o maior primo de S. Logo, S não é finito

Exercício 22.

Mostre que se $2^m + 1$ é primo para algum $m > 0$ então m é uma potência de 2.

Solução 22.
Suponha que $2^m + 1$ seja primo mas m não seja potência de 2. Logo, $m = r \cdot s$, com r par e s ímpar. Logo:

$$2^m + 1 = 2^{rs} + 1 = (2^r)^s + 1 = (2^r + 1)\left(2^{r(s-1)} - 2^{r(s-2)} - \cdots + 1\right).$$

Logo $2^r + 1 \mid 2^m + 1$

Exercício 23.
Seja $p_1 = 2, p_2 = 3, p_3 = 5, \ldots, p_n, \ldots$ a sequência dos números primos positivos em sua ordem natural.

a) Mostre que $p_{n+1} \leqslant p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$;

b) Mostre que $p_n \leqslant 2^{2^{n-1}}$, para todo $n \geqslant 1$. (*Dica:* use indução.)

c) Conclua que existem pelo menos $n + 1$ primos menores 2^{2^n}.

Solução 23.

a) Seja $\mathbb{P} = \{p_1, p_2, \cdots\}$ o conjunto dos números primos na sua ordem crescente. Pela prova de Euclides (que os primos são infinitos), temos que $p = p_1 \cdot p_2 \cdots p_n + 1$ é primo, com $p \neq p_1, p \neq p_2, \cdots p \neq p_n$. Logo $p \geqslant p_{n+1}$, que é o próximo na sucessão dos primos.

b) *Base*: $n = 1$

$$p_1 = 2 \leqslant 2^{2^{1-1}} = 2^{2^0} = 2^1 = 2$$

Hipótese: $n = k > 1$

$$p_k \leqslant 2^{2^{k-1}}$$

Passo: $n = k + 1$

$$p_{k+1} \leqslant p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1 \leqslant 2^{2^{k-1}} + 1 \leqslant 2^{2^k}$$

c) É uma conclusão direta do item anterior, pois $p_{n+1} \leqslant 2^{2^n}$, ou seja, $p_1 < p_2 < \cdots < p_n < p_{n+1} \leqslant 2^{2^k}$.

Exercício 24.
Prove que um inteiro é divisível por 3 se, e somente se, a some de seus dígitos for divisível por 3. Prove que um inteiro é divisível por 9 se, e somente se, a some de seus dígitos for divisível por 9.

Solução 24.

$$n = (a_n a_{n-1} \cdots a_1 a_0)_{10} = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10^1 + a_0 10^0$$

$$n = a_n (10^n - 1) + a_{n-1}\left(10^{n-1} - 1\right) + a_1\left(10^1 - 1\right) + (a_n + a_{n-1} + \cdots + a_1 + a_0)$$

$$10 \equiv 1 (\mathrm{mod} 9) \Rightarrow 10^n \equiv 1 (\mathrm{mod} 9)$$
$$10^n - 1 \equiv 0 (\mathrm{mod} 9) \Rightarrow 9 \mid 10^n - 1 \Rightarrow 3 \mid 10^n - 1; \forall n \in \mathbb{N}$$

$$3 \mid n \Leftrightarrow 3 \mid (a_n + a_{n-1} + \cdots + a_1 + a_0)$$
$$9 \mid n \Leftrightarrow 9 \mid (a_n + a_{n-1} + \cdots + a_1 + a_0)$$

Exercício 25.
Prove que um inteiro é divisível por 11 se, e somente se, a diferença entre a soma dos seus dígitos nas posições ímpares e a soma dos seus dígitos nas posições pares for divisível por 11.

Solução 25.

$$n = (a_n a_{n-1} \cdots a_1 a_0)_{10} = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10^1 + a_0 10^0$$

$$10 \equiv -1 (\mathrm{mod} 11) \Rightarrow \begin{cases} 10^n \equiv 1 (\mathrm{mod} 11), & \text{se n é par} \\ 10^n \equiv -1 (\mathrm{mod} 11), & \text{se n é ímpar} \end{cases}$$

$$\begin{aligned} n &\equiv a_0 - a_1 + a_2 - a_3 + \cdots (\mathrm{mod} 11) \\ &\equiv (a_0 + a_2 + a_4 + \cdots) - (a_1 + a_3 + a_5 + \cdots) (\mathrm{mod} 11) \end{aligned}$$

$$11 \mid n \Leftrightarrow 11 \mid (a_0 + a_2 + a_4 + \cdots) - (a_1 + a_3 + a_5 + \cdots)$$

Congruências

Exercício 26.

a) Encontre $x \in \mathbb{Z}$, $0 \leqslant x \leqslant 6$, tal que $11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19 \equiv x \pmod{7}$

b) Encontre $x \in \mathbb{Z}$, $0 \leqslant x \leqslant 3$, tal que $(1 + 2 + 2^2 + \cdots + 2^{19}) \equiv x \pmod{4}$

Solução 26.

a) $11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19 \equiv 4 \cdot 4 \cdot 5 \cdot 6 \cdot 5 \equiv 16 \cdot 30 \cdot 5 \equiv 2 \cdot 2 \cdot 5 \equiv 20 \equiv 6 (\mathrm{mod} 7)$.

b) $1 + 2 + 2^2 + \cdots + 2^{19} = 1 + 2 + 4 + 4 \cdot 2 + 4 \cdot 4 + \cdots + 4 \cdot 2^{17} \equiv 1 + 2 \equiv 3 (\mathrm{mod} 4)$.

Exercício 27.

Sejam a, b inteiros e r, s inteiros positivos. Prove que

$$a \equiv b \pmod{r} \Leftrightarrow as \equiv bs \pmod{rs}$$

Solução 27.

$$a \equiv b (\mathrm{mod} r) \Leftrightarrow a - b = q \cdot r \Leftrightarrow as - bs = q \cdot (rs) \Leftrightarrow as \equiv bs (\mathrm{mod} rs).$$

Exercício 28.

Sejam a, b inteiros e d, m inteiros positivos. Mostre que se $a \equiv b \pmod{m}$ e d divide m assim $a \equiv b \pmod{d}$.

Solução 28.

Se $d \mid m$, então $m = k \cdot d; k \in \mathbb{Z}$. Logo:

$$a \equiv b (\mathrm{mod} m) \Rightarrow a - b = m \cdot q \Rightarrow a - b = (qk)\, d \Rightarrow a \equiv b (\mathrm{mod} d).$$

Exercício 29.

Sejam a, b inteiros e r, s inteiros positivos. Mostre que se $a \equiv b \pmod{r}$ e $a \equiv b \pmod{s}$ então $a \equiv b \pmod{\mathrm{mmc}(r, s)}$

Solução 29.

$$\begin{cases} a \equiv b (\mathrm{mod} r) \\ a \equiv b (\mathrm{mod} s) \end{cases} \Rightarrow \begin{cases} r \mid a - b \\ s \mid a - b \end{cases}$$

Note que como $r \mid a - b$ e $s \mid a - b$, então r e s são múltiplos comuns de $a - b$. Pela definição de mmc, temos que $\mathrm{mmc}(r, s) \mid r$ e $\mathrm{mmc}(r, s) \mid s$. Logo,

$$\mathrm{mmc}(r, s) \mid a - b \Rightarrow a \equiv b (\mathrm{mod} \mathrm{mmc}(r, s)).$$

Exercício 30.
Sejam a, b inteiros e r, m inteiros positivos. Mostre que se $ra \equiv rb \pmod{m}$ e mdc$(r, m) = 1$ então $a \equiv b \pmod{m}$

Solução 30.

$$ra \equiv rb (\mathrm{mod} m) \Rightarrow m \mid ra - rb \Rightarrow m \mid r(a - b)$$

$$\text{mdc}(r, m) = 1 \Rightarrow m \nmid r.$$

Logo:

$$m \mid a - b \Rightarrow a \equiv b (\mathrm{mod} m)$$

Exercício 31.
Mostre que se $x \equiv y \pmod{m}$ assim mdc$(x, m) =$ mdc(y, m).

Solução 31.
Sejam $d =$ mdc (x, m), $d' =$ mdc (y, m). Logo $d \mid x$, $d \mid m$ e $d' \mid y$ e $d' \mid m$.

$$x \equiv y (\mathrm{mod} m) \Rightarrow x - y = m \cdot q$$

$$d \mid x \wedge d \mid m \Rightarrow d \mid y \Rightarrow d \mid d'$$

$$d' \mid y \wedge d' \mid m \Rightarrow d' \mid x \Rightarrow d' \mid d$$

$$\therefore d' = d.$$

Exercício 32.
Mostre que $6 \cdot 4^m \equiv 6 \pmod{9}$, para todo inteiro $m \geqslant 0$.

Solução 32.

$$4 \equiv 1 (\mathrm{mod} 3)$$

$$4^m \equiv 1 \pmod{3}$$

$$2 \cdot 4^m \equiv 2 \pmod{3}$$

$$6 \cdot 4^m \equiv 6 \pmod{9}$$

Exercício 33.
Mostre que $5^n + 6^n \equiv 0 \pmod{11}$ para todo inteiro positivo impar m.

Solução 33.

$$\begin{cases} 5 \equiv -1 \pmod{11} \\ 6 \equiv 1 \pmod{11} \end{cases} \Rightarrow \begin{cases} 5^n \equiv (-1)^n \pmod{11} \\ 6^n \equiv 1 \pmod{11} \end{cases} \overset{\text{n ímpar}}{\Longrightarrow} \begin{cases} 5^n \equiv -1 \pmod{11} \\ 6^n \equiv 1 \pmod{11} \end{cases} \Rightarrow$$

$$5^n + 6^n \equiv 0 \pmod{11}.$$

Exercício 34.
Seja a um inteiro. Mostre as afirmações abaixo.

a) $a^2 \equiv 0, 1$ ou $4 \pmod 8$.

b) Se a é um cubo, então a^2 é congruente a $0, 1, 9$ ou 28 modulo 36

c) Se $2 \nmid a$ e $3 \nmid a$ então $a^2 \equiv 1 \pmod{24}$.

Solução 34.

a)

$$\begin{aligned}
&a \equiv 0 \pmod 8 \Rightarrow a^2 \equiv 0 \pmod 8;\\
&a \equiv 1 \pmod 8 \Rightarrow a^2 \equiv 1 \pmod 8;\\
&a \equiv 2 \pmod 8 \Rightarrow a^2 \equiv 4 \pmod 8;\\
&a \equiv 3 \pmod 8 \Rightarrow a^2 \equiv 9 \equiv 1 \pmod 8;\\
&a \equiv 4 \pmod 8 \Rightarrow a^2 \equiv 16 \equiv 0 \pmod 8;\\
&a \equiv 5 \pmod 8 \Rightarrow a^2 \equiv 25 \equiv 1 \pmod 8;\\
&a \equiv 6 \pmod 8 \Rightarrow a^2 \equiv 36 \equiv 4 \pmod 8;\\
&a \equiv 7 \pmod 8 \Rightarrow a^2 \equiv 49 \equiv 1 \pmod 8.
\end{aligned}$$

b) Se a é cubo, então $a = n^3, n \in \mathbb{Z}$. Logo, $a^2 = n^6$. Pelo algoritmo da divisão, $n = 6k + r$, com $k \in \mathbb{Z}$ e $r \in \{0, 1, 2, 3, 4, 5\}$.

$$n^6 = (6k + r)^6$$

$$n^6 = 36\left(6^4k^6 + 6^4k^5r + 15 \cdot 6^2k^4r^2 + 20 \cdot 6k^3r^3 + 15k^2r^4 + kr^5\right) + r^6$$

$$n^6 \equiv r^6 \pmod{36}$$

- $r = 0 \Rightarrow n^6 \equiv 0^6 \equiv 0 \pmod{36}$;
- $r = 1 \Rightarrow n^6 \equiv 1^6 \equiv 1 \pmod{36}$;
- $r = 2 \Rightarrow n^6 \equiv 2^6 \equiv 64 \equiv 28 \pmod{36}$;
- $r = 3 \Rightarrow n^6 \equiv 3^6 \equiv 729 \equiv 9 \pmod{36}$;
- $r = 4 \Rightarrow n^6 \equiv 4^6 \equiv \left(2^6\right)^2 \equiv 28^2 \equiv (-8)^2 \equiv 64 \equiv 28 \pmod{36}$;
- $r = 5 \Rightarrow n^6 \equiv 5^6 \equiv 15625 \equiv 1 \pmod{36}$.

c)

$$a^2 \equiv 1 \pmod{24} \Leftrightarrow 24 \mid a^2 - 1 \Leftrightarrow 3 \mid a^2 - 1 \wedge 8 \mid a^2 - 1 \Leftrightarrow \begin{matrix} a^2 \equiv 1 \pmod 3 \\ a^2 \equiv 1 \pmod 8 \end{matrix}$$

Pelo algoritmo da divisão por 3 , temos $(a \not\equiv 0 \pmod 3)$:

- $a \equiv 1 \pmod 3 \Rightarrow a^2 \equiv 1 \pmod 3$;
- $a \equiv 2 \pmod 3 \Rightarrow a^2 \equiv 4 \equiv 1 \pmod 3$.

Pelo algoritmo da divisão por 4 , temos $(a \not\equiv 0 \pmod 4$ e $a \not\equiv 2 \pmod 4)$:

- $a \equiv 1 \pmod 4 \Rightarrow a^2 \equiv 1 \pmod 4$;
- $a \equiv 3 \pmod 4 \Rightarrow a^2 \equiv 9 \equiv 1 \pmod 4$;

Exercício 35.
Prove que $n^7 \equiv n \pmod{42}$ para todo $n \in \mathbb{Z}$.

Solução 35.
Pelo Teorema de Fermat, $n^7 \equiv n \pmod{7}$. Agora vamos provar que $n^7 \equiv n \pmod{6}$.

$$\begin{aligned}
&n \equiv 0 \pmod{6} \Rightarrow n^7 \equiv 0 \pmod{6};\\
&n \equiv 1 \pmod{6} \Rightarrow n^7 \equiv 1 \pmod{6};\\
&n \equiv 2 \pmod{6} \Rightarrow n^7 \equiv 128 \equiv 2 \pmod{6};\\
&n \equiv 3 \pmod{6} \Rightarrow n^7 \equiv 2187 \equiv 3 \pmod{6};\\
&n \equiv 4 \pmod{6} \Rightarrow n^7 \equiv 16384 \equiv 4 \pmod{6};\\
&n \equiv 5 \pmod{6} \Rightarrow n^7 \equiv 78125 \equiv 5 \pmod{6}.
\end{aligned}$$

$$\therefore n^7 \equiv n \pmod{6}.$$

$$\left.\begin{aligned} n^7 \equiv n \pmod{7} &\Rightarrow 7 \mid n^7 - n\\ n^7 \equiv n \pmod{6} &\Rightarrow 6 \mid n^7 - n \end{aligned}\right\} \Rightarrow \text{mmc}(7,6) = 42 \mid n^7 - n \Rightarrow n^7 \equiv n \pmod{42}.$$

Exercício 36.
Determine o resto das divisões de:

a) 2^{50} por 7;

b) 41^{65} por 7;

c) $(1^5 + 2^5 + \cdots + 100^5)$ por 4;

d) 57383^5 por 19.

Solução 36.

a) $2^3 \equiv 8 \equiv 1 \pmod{7} \Rightarrow \left(2^3\right)^{16} \equiv 1^{16} \pmod{7} \Rightarrow 2^{48} \cdot 2^2 \equiv 1 \cdot 4 \pmod{7} \Rightarrow 2^{50} \equiv 4 \pmod{7}$.
O resto é 4.

b) $41 \equiv -1 \pmod{7} \Rightarrow 41^{65} \equiv (-1)^{65} \pmod{7} \Rightarrow 41^{65} \equiv -1 \pmod{7} \Rightarrow 41^{65} \equiv 6 \pmod{7}$.
O resto é 6.

c) Note que:

$$\left.\begin{aligned} &1 \equiv 1 \pmod{4} \Rightarrow 1^5 \equiv 1 \pmod{4}\\ &2 \equiv 2 \pmod{4} \Rightarrow 2^5 \equiv 32 \equiv 0 \pmod{4}\\ &3 \equiv 3 \pmod{4} \Rightarrow 3^5 \equiv 243 \equiv 3 \pmod{4}\\ &4 \equiv 0 \pmod{4} \Rightarrow 4^5 \equiv 0 \pmod{4} \end{aligned}\right\} \Rightarrow 1^5 + 2^5 + 3^5 + 4^5 \equiv 0 \pmod{4}$$

E repare que o padrão se repete, pois

$$\left.\begin{aligned} &5 \equiv 1 \pmod{4} \Rightarrow 5^5 \equiv 1 \pmod{4}\\ &6 \equiv 2 \pmod{4} \Rightarrow 6^5 \equiv 32 \equiv 0 \pmod{4}\\ &7 \equiv 3 \pmod{4} \Rightarrow 7 \equiv 243 \equiv 3 \pmod{4}\\ &8 \equiv 0 \pmod{4} \Rightarrow 8^5 \equiv 0 \pmod{4} \end{aligned}\right\} \Rightarrow 5^5 + 6^5 + 7^5 + 8^5 \equiv 0 \pmod{4}$$

Logo $1^5 + 2^5 + 3^5 + \cdots + 100^5 \equiv 0\,(\mathrm{mod} 4)$.

O resto é 0.

d) $573873 \equiv 3\,(\mathrm{mod} 19) \Rightarrow 573873^5 \equiv 3^5 \equiv 243 \equiv 15\,(\mathrm{mod} 19)$.

O resto é 15.

Exercício 37.
Use congruências para verificar que:

a) $89 \mid 2^{44} - 1$;

b) $23 \mid 2^{11} - 1$.

Solução 37.

a)

$$\begin{aligned} &2^7 \equiv 128 \equiv 39\,(\mathrm{mod} 89) \\ &2^{14} \equiv 1521 \equiv 8\,(\mathrm{mod} 89) \\ &2^{42} \equiv 8^3 \equiv 512 \equiv 67\,(\mathrm{mod} 89) \\ &2^{44} \equiv 67 \cdot 4 \equiv 268 \equiv 1\,(\mathrm{mod} 89) \\ &2^{44} \equiv 1\,(\mathrm{mod} 89) \Rightarrow 89 \mid 2^{44} - 1. \end{aligned}$$

b)

$$\begin{aligned} &2^5 \equiv 32 \equiv 9\,(\mathrm{mod} 23) \\ &2^{10} \equiv 9^2 \equiv 81 \equiv 12\,(\mathrm{mod} 23) \\ &2^{11} \equiv 12 \cdot 2 \equiv 24 \equiv 1\,(\mathrm{mod} 23) \\ &2^{11} \equiv 1\,(\mathrm{mod} 23) \Rightarrow 23 \mid 2^{11} - 1. \end{aligned}$$

Exercício 38.
Resolva as seguintes congruências lineares:

a) $25x \equiv 15\ (\mathrm{mod} 29)$;

b) $140x \equiv 133\ (\mathrm{mod} 301)$.

Solução 38.

a) Como mdc $(25, 29) = 1$ e $1 \mid 15$, a congruência tem solução.

$$\begin{aligned} 25x &\equiv 15\,(\mathrm{mod} 29) \\ -4x &\equiv 15\,(\mathrm{mod} 29) \\ -28x &\equiv 105 \equiv 18\,(\mathrm{mod} 29) \\ x &\equiv 18\,(\mathrm{mod} 29) \\ x &= 18 + 29t; t \in \mathbb{Z}. \end{aligned}$$

b) Como mdc $(140, 301) = 7$ e $7 \mid 133$, a congruência tem solução.

$$\begin{aligned} 140x &\equiv 133\,(\mathrm{mod}301) \\ 20x &\equiv 19\,(\mathrm{mod}43) \\ 40x &\equiv 38 \equiv -5\,(\mathrm{mod}43) \\ -3x &\equiv -5\,(\mathrm{mod}43) \\ -42x &\equiv -70 \equiv 16\,(\mathrm{mod}43) \\ x &\equiv 16\,(\mathrm{mod}43) \\ x &= 16 + 43t; t \in \mathbb{Z}. \end{aligned}$$

Exercício 39.
Usando congruências, resolva as seguintes equações diofantinas:

a) $4x + 51y = 9$;

b) $12x + 25y = 331$.

Solução 39.
a) Como mdc $(4, 51) = 1$ e $1 \mid 9$, a congruência tem solução.

$$\begin{aligned} 4x + 51y &= 9 \\ 4x + 51y &\equiv 9\,(\mathrm{mod}4) \\ -y &\equiv 1\,(\mathrm{mod}4) \\ y &\equiv 3\,(\mathrm{mod}4) \\ y &= 3 + 4t; t \in \mathbb{Z}. \end{aligned}$$

$$\begin{aligned} 4x + 51\,(3 + 4t) &= 9 \\ 4x + 153 + 204t &= 9 \\ 4x &= -144 - 204t \\ x &= -36 - 51t. \end{aligned}$$

$$S = \{(x, y) : x = -36 - 51t \text{ e } y = 3 + 4t; t \in \mathbb{Z}\}.$$

b) Como mdc $(12, 25) = 1$ e $1 \mid 331$, a congruência tem solução.

$$\begin{aligned} 12x + 25y &= 331 \\ 2x + 25y &\equiv 331\,(\mathrm{mod}12) \\ y &\equiv 7\,(\mathrm{mod}12) \\ y &= 7 + 12t; t \in \mathbb{Z}. \end{aligned}$$

$$\begin{aligned} 12x + 25\,(7 + 12t) &= 331 \\ 12x + 175 + 300t &= 331 \\ 12x &= 156 - 300t \\ x &= 13 - 25t. \end{aligned}$$

$$S = \{(x, y) : x = 13 - 25t \text{ e } y = 7 + 12t; t \in \mathbb{Z}\}.$$

Exercício 40.
Determine todas as soluções das congruências abaixo:

a) $3x - 7y \equiv 11\,(\mathrm{mod} 13)$;

b) $17x \equiv 3\,(\mathrm{mod} 2 \cdot 3 \cdot 5 \cdot 7)$.

Solução 40.

a) $3x - 7y \equiv 11\,(\mathrm{mod} 13) \Rightarrow 3x \equiv 11 + 7y\,(\mathrm{mod} 13)$. Como $\mathrm{mdc}\,(3, 13) = 1$ e $1 \mid 11 + 7y$, o problema tem solução.

$$\begin{aligned} 3x &\equiv 11 + 7y\,(\mathrm{mod} 13) \\ x &\equiv 99 + 63y \equiv 8 - 2y\,(\mathrm{mod} 13) \end{aligned}$$

$$S = \{(x, y) : x = 8 - 2t + 13q \text{ e } y = t; t, q \in \mathbb{Z}\}.$$

b)

$$17x \equiv 3\,(\mathrm{mod} 2 \cdot 3 \cdot 5 \cdot 7) \Rightarrow \begin{cases} 17x \equiv 3\,(\mathrm{mod} 2) \\ 17x \equiv 3\,(\mathrm{mod} 3) \\ 17x \equiv 3\,(\mathrm{mod} 5) \\ 17x \equiv 3\,(\mathrm{mod} 7) \end{cases}$$

$$\begin{aligned} 17x &\equiv 3\,(\mathrm{mod} 2) \\ x &\equiv 1\,(\mathrm{mod} 2) \\ x &= 1 + 2a; a \in \mathbb{Z}. \end{aligned}$$

$$\begin{aligned} 17x &\equiv 3\,(\mathrm{mod} 3) \\ 17 + 34a &\equiv 3\,(\mathrm{mod} 3) \\ 2 + a &\equiv 0\,(\mathrm{mod} 3) \\ a &\equiv 1\,(\mathrm{mod} 3) \\ a &= 1 + 3b \\ x &= 3 + 6b; b \in \mathbb{Z}. \end{aligned}$$

$$\begin{aligned} 17x &\equiv 3\,(\mathrm{mod} 5) \\ 51 + 102b &\equiv 3\,(\mathrm{mod} 5) \\ 1 + 2b &\equiv 3\,(\mathrm{mod} 5) \\ 2b &\equiv 2\,(\mathrm{mod} 5) \\ b &\equiv 1\,(\mathrm{mod} 5) \\ b &= 1 + 5c \\ x &= 9 + 30c; c \in \mathbb{Z}. \end{aligned}$$

$$\begin{aligned} 17x &\equiv 3\,(\mathrm{mod} 7) \\ 153 + 510c &\equiv 3\,(\mathrm{mod} 7) \\ -1 + 6c &\equiv 3\,(\mathrm{mod} 7) \\ 6c &\equiv 4\,(\mathrm{mod} 7) \\ c &\equiv 24 \equiv 3\,(\mathrm{mod} 7) \\ c &= 3 + 7d \\ x &= 99 + 210d; d \in \mathbb{Z}. \end{aligned}$$

$$x \equiv 99\,(\mathrm{mod} 210)$$