Lista 4 com respostas

MAT0120 — 1° SEMESTRE DE 2020

Sistemas de Congruências Lineares

Exercício 1.
Resolva os seguintes sistemas de congruências lineares:

a) $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$,

b) $\begin{cases} x \equiv 5 \pmod 6 \\ x \equiv 4 \pmod{11} \\ x \equiv 3 \pmod 7 \end{cases}$,

c) $\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 5 \\ x \equiv 0 \pmod 7 \end{cases}$.

Solução 1.

a) Como $\text{mdc}(3,5) = \text{mdc}(3,7) = \text{mdc}(5,7) = 1$, o sistema tem solução.

$$\begin{cases} N_1 = 5 \cdot 7 = 35 \\ N_2 = 3 \cdot 7 = 21 \\ N_3 = 3 \cdot 5 = 15 \end{cases} \Rightarrow \begin{cases} 35r_1 \equiv 1 (\text{mod } 3) \\ 21r_2 \equiv 1 (\text{mod } 5) \\ 15r_3 \equiv 1 (\text{mod } 7) \end{cases} \Rightarrow \begin{cases} r_1 \equiv 2 (\text{mod } 3) \\ r_2 \equiv 1 (\text{mod } 5) \\ r_3 \equiv 1 (\text{mod } 7) \end{cases}$$

$$x \equiv 35 \cdot 2 \cdot 1 + 21 \cdot 1 \cdot 2 + 15 \cdot 1 \cdot 3 (\text{mod } 3 \cdot 5 \cdot 7)$$

$$x \equiv 157 \equiv 52 (\text{mod } 105).$$

b) Como $\text{mdc}(6,11) = \text{mdc}(6,7) = \text{mdc}(11,7) = 1$, o sistema tem solução.

$$\begin{cases} N_1 = 11 \cdot 7 = 77 \\ N_2 = 6 \cdot 7 = 42 \\ N_3 = 6 \cdot 11 = 66 \end{cases} \Rightarrow \begin{cases} 77r_1 \equiv 1 (\text{mod } 6) \\ 42r_2 \equiv 1 (\text{mod } 11) \\ 66r_3 \equiv 1 (\text{mod } 7) \end{cases} \Rightarrow \begin{cases} r_1 \equiv 5 (\text{mod } 6) \\ r_2 \equiv 5 (\text{mod } 11) \\ r_3 \equiv 5 (\text{mod } 7) \end{cases}$$

$$x \equiv 77 \cdot 5 \cdot 5 + 42 \cdot 5 \cdot 4 + 66 \cdot 5 \cdot 3 (\text{mod } 6 \cdot 11 \cdot 7)$$

$$x \equiv 3755 \equiv 59 (\text{mod } 462).$$

c) Como $\text{mdc}(2,3) = \text{mdc}(2,5) = \text{mdc}(2,7) = \text{mdc}(3,5) = \text{mdc}(3,7) = \text{mdc}(5,7) = 1$, o sistema tem solução.

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 5 \\ x \equiv 0 \pmod 7 \end{cases} \Rightarrow \begin{cases} x \equiv -1 \pmod 2 \\ x \equiv -1 \pmod 3 \\ x \equiv -1 \pmod 5 \\ x \equiv 0 \pmod 7 \end{cases} \Rightarrow \begin{cases} x \equiv -1 \pmod{2 \cdot 3 \cdot 5} \\ x = 7k \end{cases}$$

$$7k \equiv -1 (\text{mod } 30) \Rightarrow k \equiv -13 (\text{mod } 30) \Rightarrow k \equiv 17 (\text{mod } 30) \Rightarrow k = 17 + 30p$$
$$x = 7k = 119 + 210p \Rightarrow x \equiv 119 (\text{mod } 210).$$

Exercício 2.
Resolva os seguintes sistemas de congruências lineares:

a) $\begin{cases} 4x \equiv 3 \ (\text{mod } 7) \\ 5x \equiv 4 \ (\text{mod } 11) \\ 11x \equiv 8 \ (\text{mod } 13) \end{cases}$,

b) $\begin{cases} 3x \equiv 5 \ (\text{mod } 2) \\ x \equiv -3 \ (\text{mod } 5) \\ 4x \equiv 7 \ (\text{mod } 9) \end{cases}$.

Solução 2.

a)
$$\begin{cases} 4x \equiv 3 \ (\text{mod } 7) \\ 5x \equiv 4 \ (\text{mod } 11) \\ 11x \equiv 8 \ (\text{mod } 13) \end{cases} \Rightarrow \begin{cases} x \equiv 6 \ (\text{mod } 7) \\ x \equiv 3 \ (\text{mod } 11) \\ x \equiv 9 \ (\text{mod } 13) \end{cases}$$

Como $\text{mdc}(7, 11) = \text{mdc}(7, 13) = \text{mdc}(11, 13) = 1$, o sistema tem solução.

$$\begin{cases} N_1 = 11 \cdot 13 = 143 \\ N_2 = 7 \cdot 13 = 91 \\ N_3 = 7 \cdot 11 = 77 \end{cases} \Rightarrow \begin{cases} 143r_1 \equiv 1 (\text{mod } 7) \\ 91r_2 \equiv 1 (\text{mod } 11) \\ 77r_3 \equiv 1 (\text{mod } 13) \end{cases} \Rightarrow \begin{cases} r_1 \equiv 5 (\text{mod } 7) \\ r_2 \equiv 4 (\text{mod } 11) \\ r_3 \equiv 12 (\text{mod } 13) \end{cases}$$
$$x \equiv 143 \cdot 5 \cdot 6 + 91 \cdot 4 \cdot 3 + 77 \cdot 12 \cdot 9 (\text{mod } 7 \cdot 11 \cdot 13)$$
$$x \equiv 13698 \equiv 685 (\text{mod } 1001).$$

b)
$$\begin{cases} 3x \equiv 5 \ (\text{mod } 2) \\ x \equiv -3 \ (\text{mod } 5) \\ 4x \equiv 7 \ (\text{mod } 9) \end{cases} \Rightarrow \begin{cases} x \equiv 5 \ (\text{mod } 2) \\ x \equiv 2 \ (\text{mod } 5) \\ x \equiv 4 \ (\text{mod } 9) \end{cases}$$

Como $\text{mdc}(2, 5) = \text{mdc}(5, 9) = \text{mdc}(2, 9) = 1$, o sistema tem solução.

$$\begin{cases} N_1 = 5 \cdot 9 = 45 \\ N_2 = 2 \cdot 9 = 18 \\ N_3 = 2 \cdot 5 = 10 \end{cases} \Rightarrow \begin{cases} 45r_1 \equiv 1 (\text{mod } 2) \\ 18r_2 \equiv 1 (\text{mod } 5) \\ 10r_3 \equiv 1 (\text{mod } 9) \end{cases} \Rightarrow \begin{cases} r_1 \equiv 1 (\text{mod } 2) \\ r_2 \equiv 2 (\text{mod } 5) \\ r_3 \equiv 1 (\text{mod } 9) \end{cases}$$
$$x \equiv 45 \cdot 1 \cdot 5 + 18 \cdot 2 \cdot 2 + 10 \cdot 1 \cdot 4 (\text{mod } 2 \cdot 5 \cdot 9)$$
$$x \equiv 337 \equiv 67 \equiv (\text{mod } 90).$$

Exercício 3.
Determine o menor inteiro a, maior que 100, tal que:

$$2 \mid a;\ 3 \mid (a+1);\ 4 \mid (a+2);\ 5 \mid (a+3);\ 6 \mid (a+4).$$

Solução 3.

$$\begin{cases} a \equiv 0 (\mathrm{mod}\ 2) \\ a \equiv -1 (\mathrm{mod}\ 3) \\ a \equiv -2 (\mathrm{mod}\ 4) \\ a \equiv -3 (\mathrm{mod}\ 5) \\ a \equiv -4 (\mathrm{mod}\ 6) \end{cases} \Rightarrow \begin{cases} a \equiv 0 (\mathrm{mod}\ 2) \\ a \equiv 2 (\mathrm{mod}\ 3) \\ a \equiv 2 (\mathrm{mod}\ 4) \\ a \equiv 2 (\mathrm{mod}\ 5) \\ a \equiv 2 (\mathrm{mod}\ 6) \end{cases} \Rightarrow \begin{cases} a \equiv 0 (\mathrm{mod}\ 2) \\ a \equiv 2 (\mathrm{mod}\ \mathrm{mmc}(3,4,5,6)) \end{cases} \Rightarrow$$

$$\begin{cases} a \equiv 0 (\mathrm{mod}\ 2) \\ a \equiv 2 (\mathrm{mod}\ 60) \end{cases} \Rightarrow \begin{cases} a = 2k \\ 2k \equiv 2 (\mathrm{mod}\ 60) \end{cases} \Rightarrow \begin{cases} a = 2k \\ k \equiv 1 (\mathrm{mod}\ 30) \end{cases} \Rightarrow a \equiv 2 (\mathrm{mod}\ 60).$$

Portanto $a = 2 + 2 \cdot 60 = 122$.

Exercício 4.
Se de uma cesta com ovos retiramos duas unidades por vez, sobra 1 ovo. O mesmo acontece se os ovos são retirados de 3 em 3, de 4 em 4, de 5 em 5, de 6 em 6. Mas não resta nenhum resto se retiramos 7 unidades cada vez. Qual é menor numero possível de ovos na cesta?

Solução 4.
Seja x o número de ovos. Então:

$$\begin{cases} x \equiv 1 (\mathrm{mod}\ 2) \\ x \equiv 1 (\mathrm{mod}\ 3) \\ x \equiv 1 (\mathrm{mod}\ 4) \\ x \equiv 1 (\mathrm{mod}\ 5) \\ x \equiv 1 (\mathrm{mod}\ 6) \\ x \equiv 0 (\mathrm{mod}\ 7) \end{cases} \Rightarrow \begin{cases} x \equiv 1 (\mathrm{mod}\ \mathrm{mmc}(2,3,4,5,6)) \\ x \equiv 0 (\mathrm{mod}\ 7) \end{cases} \Rightarrow \begin{cases} x \equiv 1 (\mathrm{mod}\ 60) \\ x \equiv 0 (\mathrm{mod}\ 7) \end{cases} \Rightarrow$$

$$\begin{cases} 7k \equiv 1 (\mathrm{mod}\ 60) \\ x = 7k \end{cases} \Rightarrow \begin{cases} k \equiv 43 (\mathrm{mod}\ 60) \\ x = 7k \end{cases} \Rightarrow x \equiv 301 (\mathrm{mod}\ 60).$$

Portanto, são 301 ovos.

Teoremas de Euler, Fermat e Wilson

Exercício 5.
Seja a um inteiro. Demonstre as afirmações abaixo.

a) $a^{21} \equiv a \pmod{15}$;

b) Se $\text{mdc}(a, 35) = 1$ então $a^{12} = 1 \pmod{35}$;

c) Se $\text{mdc}(a, 42) = 1$ então $3 \cdot 7 \cdot 8 \mid a^6 - 1$.

Solução 5.

a) $a^{21} \equiv a \pmod{15} \Leftrightarrow a^{21} \equiv a \pmod{3}$ e $a^{21} \equiv a \pmod{5}$.

Pelo Teorema de Fermat, temos:

$$a^{21} = (a^3)^7 \equiv a^7 = a^3 \cdot a^3 \cdot a \equiv a \cdot a \cdot a = a^3 \equiv a (\text{mod } 3).$$

Novamente, pelo Teorema de Fermat:

$$a^{21} = (a^5)^4 \cdot a \equiv a^4 \cdot a = a^5 \equiv a (\text{mod } 5).$$

b) $\text{mdc}(a, 35) = 1 \Leftrightarrow \text{mdc}(a, 5) = \text{mdc}(a, 7) = 1$.

Como $7 \nmid a$, pelo Teorema de Fermat, temos:

$$a^6 \equiv 1 (\text{mod } 7)$$

$$a^{12} = (a^6)^2 \equiv 1^2 \equiv 1 (\text{mod } 7).$$

Como $5 \nmid a$, pelo Teorema de Fermat, temos:

$$a^4 \equiv 1 (\text{mod } 5)$$

$$a^{12} = (a^4)^3 \equiv 1^3 \equiv 1 (\text{mod } 5).$$

c) $\text{mdc}(a, 42) = 1 \Leftrightarrow \text{mdc}(a, 2) = \text{mdc}(a, 3) = \text{mdc}(a, 7) = 1$, pois $2, 3$ e 7 são coprimos. Como $3 \nmid a$ e $7 \nmid a$, então, pelo Teorema de Fermat, temos:

$$a^2 \equiv 1 (\text{mod } 3) \Rightarrow a^6 = (a^2)^3 \equiv 1^3 = 1 (\text{mod } 3) \Rightarrow 3 \mid a^6 - 1$$

e

$$a^6 \equiv 1 (\text{mod } 7) \Rightarrow 7 \mid a^6 - 1.$$

Falta provar que $8 \mid a^6 - 1$.

Note que $a^6 - 1 = (a + 1)(a - 1)(a^2 - a + 1)(a^2 + a + 1)$. Como $\text{mdc}(a, 2) = 1$, então a é ímpar. Tomando $a = 2k + 1$, temos:

$$a^6 - 1 = 4k(k + 1)(4k^2 + 2k + 1)(4k^2 + 6k + 3).$$

No entanto, k e $k + 1$ tem paridades distintas, ou seja, um deles é par. Assim, $8 \mid a^6 - 1$.

Logo, $3 \cdot 7 \cdot 8 \mid a^6 - 1$.

Exercício 6.

a) Sejam a, b inteiros e seja p um primo positivo tal que $\text{mdc}(a, p) = 1$. Mostre que $x = a^{p-2}b$ é solução da congruência $ax \equiv b \pmod{p}$.

b) Resolva as congruências $6x \equiv 5 \pmod{11}$ e $3x \equiv 17 \pmod{29}$

Solução 6.

a) Como $p \nmid a$, temos que $a^{p-1} \equiv 1 (\text{mod } p)$. Assim:

$$a \cdot (a^{p-2}b) = a^{p-1}b \equiv 1 \cdot b = b (\text{mod } p).$$

b) Como $\text{mdc}(6, 11) = 1$ e $1 \mid 5$, a equação tem solução:

$$\begin{aligned} 6x &\equiv 5 (\text{mod } 11) \\ 12x &\equiv 10 (\text{mod } 11) \\ x &\equiv 10 (\text{mod } 11). \end{aligned}$$

Como $\text{mdc}(3, 29) = 1$ e $1 \mid 17$, a equação tem solução:

$$\begin{aligned} 3x &\equiv 17 (\text{mod } 29) \\ 30x &\equiv 170 (\text{mod } 29) \\ x &\equiv 25 (\text{mod } 29). \end{aligned}$$

Exercício 7.

Encontre o resto da divisão de

a) 5^{14} por 7.

b) 5^{100} por 11.

c) 15^{175} por 11.

d) 31^{200} por 28.

e) $2^{7^{2002}}$ por 352.

Solução 7.

a) Pelo Teorema de Fermat, temos:

$$\begin{aligned} 5^7 &\equiv 5 (\text{mod } 7) \\ (5^7)^2 &\equiv 5^2 (\text{mod } 7) \\ 5^{14} &\equiv 25 \equiv 4 (\text{mod } 7) \end{aligned}$$

O resto é 4.

b) Pelo Teorema de Fermat, temos:

$$\begin{aligned} 5^{10} &\equiv 1 (\text{mod } 11) \\ (5^{10})^{10} &\equiv 1^{10} (\text{mod } 11) \\ 5^{100} &\equiv 1 (\text{mod } 11) \end{aligned}$$

O resto é 1.

c) Pelo Teorema de Fermat, temos:

$$\begin{aligned} 15^{10} &\equiv 1(\text{mod } 11) \\ (5^{10})^{17} &\equiv 1^{10}(\text{mod } 11) \\ 5^{170} &\equiv 1(\text{mod } 11) \\ 5^{170} \cdot 5^5 &\equiv 3125(\text{mod } 11) \\ 5^{175} &\equiv 1(\text{mod } 11) \end{aligned}$$

O resto é 1.

d) Como $\text{mdc}(31, 28) = 1$, pelo Teorema de Euler, temos que $\varphi(28) = \varphi(2^2 \cdot 7) = \varphi(2^2) \cdot \varphi(7) = (2^2 - 2) \cdot (7 - 1) = 12$. Como $31^{12k} \equiv 1(\text{mod } 28)$, precisamos achar o resto da divisão de 200 por 12. Assim:

$$31^{200} \equiv 3^{200} \equiv 3^{12 \cdot 16 + 8} \equiv 3^8 \equiv 3^3 \cdot 3^3 \cdot 3^2 \equiv (-1) \cdot (-1) \cdot 9 \equiv 9(\text{mod } 28).$$

O resto é 9.

e) Como $352 = 2^5 \cdot 11$ e $\text{mdc}(32, 11) = 1$, então, pelo Teorema Chinês dos Restos, devemos achar x tal que:

$$\begin{cases} x \equiv 2^{7^{2002}}(\text{mod } 32) \\ x \equiv 2^{7^{2002}}(\text{mod } 11) \end{cases}.$$

A primeira congruência tem solução $x \equiv 0(\text{mod } 32)$. Para resolver a segunda congruência, vamos utilizar o Teorema de Euler. Como $\varphi(11) = 11 - 1 = 10$, temos que $2^{10k} \equiv 1(\text{mod } 11)$. Assim, precisamos achar o resto da divisão de 7^{2002} por 10.

$$7^{2002} = 49^{1001} \equiv (-1)^{1001} \equiv -1 \equiv 9(\text{mod } 10).$$

Portanto,

$$2^{7^{2002}} \equiv 2^{10k+9} \equiv 2^9 \equiv 6(\text{mod } 11).$$

Logo:

$$\begin{cases} x \equiv 0(\text{mod } 32) \\ x \equiv 6(\text{mod } 11) \end{cases} \Rightarrow \begin{cases} x = 32k \\ 32k \equiv 6(\text{mod } 11) \end{cases} \Rightarrow \begin{cases} x = 32k \\ k = 5 + 11t \end{cases} \Rightarrow x \equiv 160(\text{mod } 352).$$

O resto é 160.

Exercício 8.

Encontre os dois últimos dígitos de

a) 2^{999};

b) 3^{999};

c) 5^{2020};

d) 7^{2019};

e) 123^{2010};

f) 557^{2012};

Solução 8.
Os últimos dois algarismos é dado pela divisão destes números por 100.

a) Como $100 = 2^2 \cdot 5^2$ e mdc$(4, 25) = 1$, então, pelo Teorema Chinês dos Restos, devemos achar x tal que:

$$\begin{cases} x \equiv 2^{999} (\text{mod } 4) \\ x \equiv 2^{999} (\text{mod } 25) \end{cases}.$$

A primeira congruência tem solução $x \equiv 0 (\text{mod } 4)$. Para resolver a segunda congruência, vamos utilizar o Teorema de Euler. Como $\varphi(25) = \varphi(5^2) = 5^2 - 5 = 20$, temos que $2^{20k} \equiv 1 (\text{mod } 5)$. Assim, precisamos achar o resto da divisão de 999 por 20.

$$999 = 20 \cdot 49 + 19.$$

Portanto,

$$2^{999} \equiv 2^{20 \cdot 49 + 19} \equiv 2^{19} \equiv 1024 \cdot 512 \equiv -1 \cdot 12 \equiv 13 (\text{mod } 25).$$

Logo:

$$\begin{cases} x \equiv 0 (\text{mod } 4) \\ x \equiv 13 (\text{mod } 25) \end{cases} \Rightarrow \begin{cases} x = 4k \\ 4k \equiv 13 (\text{mod } 25) \end{cases} \Rightarrow \begin{cases} x = 4k \\ k = 22 + 25t \end{cases} \Rightarrow x \equiv 88 (\text{mod } 100).$$

O resto é 88.

b) Como $\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2) = (2^2 - 2) \cdot (5^2 - 5) = 40$. Pelo Teorema de Euler, $3^{40k} \equiv 1 (\text{mod } 100)$. Note que $1000 = 40 \cdot 25$. Portanto,

$$\begin{aligned} 3^{1000} \equiv 3^{40 \cdot 25} &\equiv 1 (\text{mod } 100) \\ 3 \cdot 3^{999} &\equiv 1 (\text{mod } 100) \\ 67 \cdot 3 \cdot 3^{999} &\equiv 1 \cdot 67 (\text{mod } 100) \\ 3^{999} &\equiv 67 (\text{mod } 100). \end{aligned}$$

O resto é 67.

c) Como $100 = 2^2 \cdot 5^2$ e mdc$(4, 25) = 1$, então, pelo Teorema Chinês dos Restos, devemos achar x tal que:

$$\begin{cases} x \equiv 5^{2020} (\text{mod } 4) \\ x \equiv 5^{2020} (\text{mod } 25) \end{cases}.$$

A segunda congruência tem solução $x \equiv 0 (\text{mod } 25)$. Para resolver a primeira congruência, temos que $5 \equiv 1 (\text{mod } 4)$, logo $5^{2020} \equiv 1 (\text{mod } 4)$ Portanto, Logo:

$$\begin{cases} x \equiv 1 (\text{mod } 4) \\ x \equiv 0 (\text{mod } 25) \end{cases} \Rightarrow \begin{cases} x = 25k \\ 25k \equiv 1 (\text{mod } 4) \end{cases} \Rightarrow \begin{cases} x = 25k \\ k = 1 + 4t \end{cases} \Rightarrow x \equiv 25 (\text{mod } 100).$$

O resto é 25.

d) Como $\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2) = (2^2 - 2) \cdot (5^2 - 5) = 40$. Pelo Teorema de Euler, $7^{40k} \equiv 1 (\text{mod } 100)$. Assim, precisamos achar o resto da divisão de 2019 por 40.

$$2019 = 40 \cdot 50 + 19.$$

Portanto,

$$7^{2019} \equiv 7^{40 \cdot 50 + 19} \equiv 7^{19} (\text{mod } 100).$$

$$\left(7^4\right)^4 \cdot 7^3 \equiv 7^3 \equiv 343 \equiv 43 (\text{mod } 100)$$

O resto é 43.

e) Como $\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2) = (2^2 - 2) \cdot (5^2 - 5) = 40$. Pelo Teorema de Euler, $123^{40k} \equiv 1 (\text{mod } 100)$. Assim, precisamos achar o resto da divisão de 2010 por 40.

$$2010 = 40 \cdot 50 + 10.$$

Portanto,

$$123^{2010} \equiv 123^{40 \cdot 50 + 10} \equiv 123^{10} \equiv 23^{10} (\text{mod } 100).$$

$$\left(23^2\right)^5 \equiv 29^5 \equiv 20511149 \equiv 49 (\text{mod } 100)$$

O resto é 49.

f) Como $\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2) = (2^2 - 2) \cdot (5^2 - 5) = 40$. Pelo Teorema de Euler, $557^{40k} \equiv 1 (\text{mod } 100)$. Assim, precisamos achar o resto da divisão de 2012 por 40.

$$2012 = 40 \cdot 50 + 12.$$

Portanto,

$$557^{2012} \equiv 557^{40 \cdot 50 + 12} \equiv 557^{12} \equiv 57^{12} (\text{mod } 100).$$

$$\left(57^2\right)^6 \equiv 49^6 \equiv \left(49^2\right)^3 \equiv 1^3 \equiv 1 (\text{mod } 100)$$

O resto é 1.

Exercício 9.

a) Seja p um inteiro primo e sejam a, b inteiros arbitrários. Mostre que se $a^p \equiv b^p \pmod p$ então $a \equiv b \pmod p$.

b) Seja $p > 2$ um primo. Mostre que

$$1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod p.$$

Solução 9.

a) $a^p \equiv b^p \pmod p \Rightarrow a^p - b^p \equiv 0 (\text{mod } p)$. Pelo Teorema de Fermat, temos:

$$\begin{cases} a^p \equiv a (\text{mod } p) \\ b^p \equiv b (\text{mod } p) \end{cases} \Rightarrow a^p - b^p \equiv a - b (\text{mod } p) \Rightarrow 0 \equiv a - b (\text{mod } p) \Rightarrow a \equiv b (\text{mod } p).$$

b) Pelo Teorema de Fermat, temos:

$$\begin{cases} 1^p \equiv 1 (\text{mod } p) \\ 2^p \equiv 2 (\text{mod } p) \\ 3^p \equiv 3 (\text{mod } p) \\ \vdots \\ (p-1)^p \equiv p - 1 (\text{mod } p) \end{cases} \Rightarrow 1^p + 2^p + \cdots + (p-1)^p \equiv 1 + 2 + \cdots + p - 1 = p \cdot \left(\frac{p-1}{2}\right) \equiv 0 (\text{mod } p).$$

Note que se p é primo maior que 2, então p é ímpar, $p - 1$ é par e $\dfrac{p-1}{2} \in \mathbb{Z}$.

Exercício 10.
Mostre que $2^8 \equiv 1 \pmod{17}$ e que $2^{16} \equiv 1 (\text{mod } 17)$.

Solução 10.

$$2^8 = (2^4)^2 = 16^2 \equiv (-1)^2 \equiv 1 (\text{mod } 17);$$
$$2^{16} = (2^8)^2 \equiv 1^2 \equiv 1 (\text{mod } (17).$$

Exercício 11.
Sejam p um primo e a um inteiro tal que $p \nmid a$. Prove que

a) se $p > 2$, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ou $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$;

b) o menor inteiro positivo e tal que $a^e \equiv 1 \pmod{p}$ é divisor de $p - 1$;

c) se e é o inteiro acima de x é um inteiro tal que $a^x \equiv 1 \pmod{p}$ então $e \mid x$.

Solução 11.

a) Pelo Teorema de Fermat, temos que $a^{p-1} \equiv 1 (\text{mod } p)$. Note que $a^{p-1} = \left(a^{\frac{p-1}{2}}\right)^2$. Assim:

$$\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 (\text{mod } p) \Rightarrow \left(a^{\frac{p-1}{2}}\right)^2 - 1 \equiv 0 (\text{mod } p) \Rightarrow$$

$$\left(a^{\frac{p-1}{2}} - 1\right) \cdot \left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 (\text{mod } p) \Rightarrow p \mid \left(a^{\frac{p-1}{2}} - 1\right) \cdot \left(a^{\frac{p-1}{2}} + 1\right)$$

Se $p \mid \left(a^{\frac{p-1}{2}} - 1\right) \cdot \left(a^{\frac{p-1}{2}} + 1\right)$, então p divide um dos fatores, pois é primo. Logo:

$$\begin{cases} p \mid a^{\frac{p-1}{2}} - 1 \\ \quad \vee \\ p \mid a^{\frac{p-1}{2}} + 1 \end{cases} \Rightarrow \begin{cases} a^{\frac{p-1}{2}} \equiv 1 (\text{mod } p) \\ \quad \vee \\ a^{\frac{p-1}{2}} \equiv -1 (\text{mod } p) \end{cases}.$$

b) Pelo algoritmo da divisão por e, temos que $p - 1 = e \cdot k + r$, com $0 \leqslant r < e$ e $k \in \mathbb{Z}$. Assim:

$$a^{p-1} = a^{e \cdot k + r} = (a^e)^k \cdot a^r \equiv 1 \cdot a^r (\text{mod } p).$$

Mas $a^{p-1} \equiv 1 (\text{mod } p)$, ou seja, $a^r \equiv 1 (\text{mod } p)$, e e é o menor inteiro positivo tal que $a^e \equiv 1 (\text{mod } p)$, logo, $r = 0$, e $p - 1 = e \cdot k$. Portanto, $e \mid p - 1$.

c) Aplicando o algoritmo da divisão por e novamente, temos que $x = e \cdot k + r$, com $0 \leqslant r < e$ e $k \in \mathbb{Z}$. Assim:

$$a^x = a^{e \cdot k + r} = (a^e)^k \cdot a^r \equiv 1 \cdot a^r (\text{mod } p).$$

Mas $a^x \equiv 1 (\text{mod } p)$, ou seja, $a^r \equiv 1 (\text{mod } p)$, e e é o menor inteiro positivo tal que $a^e \equiv 1 (\text{mod } p)$, logo, $r = 0$, e $x = e \cdot k$. Portanto, $e \mid x$.

Exercício 12.

a) Sejam p, q primos distintos e impares tais que $(p-1) \mid (q-1)$. Mostre que se $\text{mdc}(a, pq) = 1$ então $a^{q-1} \equiv 1 \pmod{pq}$.

b) Seja a um inteiro. Prove que $a^{37} \equiv a \pmod{1729}$; $a^{79} \equiv a \pmod{158}$.

Solução 12.

a) Como p e q são primos, então $\text{mdc}(p, q) = 1$. Como $p-1 \mid q-1$, então $q-1 = k(p-1), k \in \mathbb{Z}$. Logo, pelo Teorema de Euler, temos:

$$\begin{aligned} a^{(p-1)} &\equiv 1 (\text{mod } p) \\ \left(a^{(p-1)}\right)^k &\equiv 1^k (\text{mod } p) \\ a^{(q-1)} &\equiv 1 (\text{mod } p). \end{aligned}$$

Novamente, pelo Teorema de Fermat, temos:

$$a^{(q-1)} \equiv 1 (\text{mod } q).$$

Assim:

$$\begin{cases} a^{(q-1)} \equiv 1 (\text{mod } p) \\ a^{(q-1)} \equiv 1 (\text{mod } q) \end{cases} \Rightarrow a^{(q-1)} \equiv 1 (\text{mod mmc}(p, q)) \Rightarrow a^{(q-1)} \equiv 1 (\text{mod } pq).$$

b) Note que $1729 = 7 \cdot 13 \cdot 19$. Pelo Teorema de Fermat, temos:

$$\begin{aligned} a^{37} = (a^7)^5 \cdot a^2 \equiv a^5 \cdot a^2 \equiv a^7 &\equiv a (\text{mod } 7) \\ a^{37} = (a^{13})^2 \cdot a^{11} \equiv a^2 \cdot a^{11} \equiv a^{13} &\equiv a (\text{mod } 13) \\ a^{37} = a^{19} \cdot a^{18} \equiv a \cdot a^{18} \equiv a^{19} &\equiv a (\text{mod } 7). \end{aligned}$$

Assim:

$$\begin{cases} a^{37} \equiv a (\text{mod } 7) \\ a^{37} \equiv a (\text{mod } 13) \\ a^{37} \equiv a (\text{mod } 19) \end{cases} \Rightarrow a^{37} \equiv a (\text{mod mmc}(7, 13, 19)) \equiv a (\text{mod } 1729).$$

Note que $158 = 79 \cdot 2$. Note que $2 \mid a^{79} - a$ pois a^{79} e a tem a mesma paridade. Logo, $a^{79} \equiv a (\text{mod } 2)$. Pelo Teorema de Fermat, temos que $a^{79} \equiv a (\text{mod } 79)$. Portanto

$$\begin{cases} a^{79} \equiv a (\text{mod } 2) \\ a^{79} \equiv a (\text{mod } 79) \end{cases} \Rightarrow a^{79} \equiv a (\text{mod mmc}(2, 79)) \equiv a (\text{mod } 158).$$

Exercício 13.

Sejam a um inteiro e n um inteiro positivo tais que $\text{mdc}(a, n) = \text{mdc}(a-1, n) = 1$. Prove que

$$1 + a + \cdots + a^{\varphi(n)-1} \equiv 0 \pmod{n}.$$

Solução 13.
Pela soma da série geométrica, temos:

$$\left(1 + a + \cdots + a^{\varphi(n)-1}\right) \cdot (a - 1) = a^{\varphi(n)} - 1,$$

ou seja,

$$\left(1 + a + \cdots + a^{\varphi(n)-1}\right) \cdot (a - 1) \equiv a^{\varphi(n)} - 1 (\text{mod } n).$$

Como $\text{mdc}(a, n) = 1$, pelo Teorema de Euler, temos que $a^{\varphi(n)} \equiv 1 (\text{mod } n)$, logo $a^{\varphi(n)} - 1 \equiv 0 (\text{mod } n)$. Assim, $\left(1 + a + \cdots + a^{\varphi(n)-1}\right) \cdot (a - 1) \equiv 0 (\text{mod } n)$.

Como $\text{mdc}(a - 1, n) = 1$, então $n \nmid a - 1$, logo $a - 1 \not\equiv 0 (\text{mod } n)$. Portanto, $1 + a + \cdots + a^{\varphi(n)-1} \equiv 0 (\text{mod } n)$.

Exercício 14.
Sejam m, n inteiros positivos relativamente primos. Prove que

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \ (\text{mod } mn).$$

Solução 14.
Como $\text{mdc}(m, n) = 1$, então $m^{\varphi(n)} \equiv 1 (\text{mod } n)$. Além disso, $n^{\varphi(m)} \equiv 0 (\text{mod } n)$. Logo:

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 (\text{mod } n).$$

Analogamente,

$$n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 (\text{mod } m).$$

Portanto:

$$\begin{cases} m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 (\text{mod } n) \\ m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 (\text{mod } m) \end{cases} \Rightarrow m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 (\text{mod mmc}(m, n)) \Rightarrow$$

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 (\text{mod } mn).$$

Exercício 15.
Determine o resto da divisão de a por b nos casos

a) $a = 15!$ e $b = 17$.

b) $a = 2 \cdot (26)!$ e $b = 29$.

Solução 15.
a) Pelo Teorema de Wilson, temos:

$$\begin{aligned} 16! &\equiv -1 (\text{mod } 17) \\ 16 \cdot 15! &\equiv -1 (\text{mod } 17) \\ -1 \cdot 15! &\equiv -1 (\text{mod } 17) \\ 15! &\equiv 1 (\text{mod } 17) \end{aligned}$$

Logo, o resto é 1.

b) Pelo Teorema de Wilson, temos:

$$\begin{aligned} 28! &\equiv -1 (\text{mod } 29) \\ 28 \cdot 27 \cdot 26! &\equiv -1 (\text{mod } 29) \\ (-1) \cdot (-2) \cdot 26! &\equiv -1 (\text{mod } 29) \\ 2 \cdot 26! &\equiv -1 (\text{mod } 29) \\ 2 \cdot 26! &\equiv 28 (\text{mod } 29) \end{aligned}$$

Logo, o resto é 28.

Exercício 16.
Reúna os inteiros $2, 3, \ldots, 21$ em pares (a, b) tais que $ab \equiv 1 \pmod{23}$.

Solução 16.

$$(2, 12), (3, 8), (4, 6), (5, 14), (6, 4), (7, 10), (8, 3), (9, 18), (10, 7), (11, 21), (12, 2)$$
$$(13, 16), (14, 5), (15, 20), (16, 13), (17, 19), (18, 9), (19, 17), (20, 15), (21, 11), (22, 22)$$

Exercício 17.
Mostre que $18! \equiv -1 (\text{mod } 437)$.

Solução 17.
Note que $437 = 23 \cdot 19$. Pelo Teorema de Wilson, $18! \equiv -1 (\text{mod } 19)$. Além disso, considerando os inversos multiplicativos do exercício anterior, temos:

$$\begin{aligned} 18! &\equiv 18 \cdot 17 \cdots 3 \cdot 2 \pmod{23} \\ 18! &\equiv 17 \cdot 15 \cdot 11 \pmod{23} \\ 18! &\equiv 17 \cdot 165 \pmod{23} \\ 18! &\equiv 17 \cdot 4 \pmod{23} \\ 18! &\equiv 68 \pmod{23} \\ 18! &\equiv -1 \pmod{23}. \end{aligned}$$

Assim:

$$\begin{cases} 18! \equiv -1 (\text{mod } 19) \\ 18! \equiv -1 (\text{mod } 23) \end{cases} \Rightarrow 18! \equiv -1 (\text{mod mmc}(19, 23)) \Rightarrow 18! \equiv -1 (\text{mod } 437).$$

Exercício 18.
Encontre o resto da divisão de

a) $5! \cdot 25!$ por 31;

b) $97!$ por 101;

c) $65!$ por 71;

d) $53!$ por 61;

e) $149!$ por 139;

Solução 18.
Pelo Teorema de Wilson, temos:

a)

$$\begin{aligned} 30! &\equiv -1 (\text{mod } 31) \\ 30 \cdot 29 \cdot 28 \cdot 27 \cdot 26 \cdot 25! &\equiv -1 (\text{mod } 31) \\ (-1) \cdot (-2) \cdot (-3) \cdot (-4) \cdot (-5) \cdot 25! &\equiv -1 (\text{mod } 31) \\ -5! \cdot 25! &\equiv -1 (\text{mod } 31) \\ 5! \cdot 25! &\equiv 1 (\text{mod } 31) \end{aligned}$$

Logo, o resto é 1.

b)

$$\begin{aligned} 100! &\equiv -1 (\text{mod } 101) \\ 100 \cdot 99 \cdot 98 \cdot 97! &\equiv -1 (\text{mod } 101) \\ (-1) \cdot (-2) \cdot (-3) \cdot 97! &\equiv -1 (\text{mod } 101) \\ 2 \cdot 3 \cdot 97! &\equiv 1 (\text{mod } 101) \\ 2 \cdot 51 \cdot 3 \cdot 34 \cdot 97! &\equiv 51 \cdot 34 (\text{mod } 101) \\ 97! &\equiv 17 (\text{mod } 101) \end{aligned}$$

Logo, o resto é 17.

c)

$$\begin{aligned} 70! &\equiv -1 (\text{mod } 71) \\ 70 \cdot 69 \cdot 68 \cdot 67 \cdot 66 \cdot 65! &\equiv -1 (\text{mod } 71) \\ (-1) \cdot (-2) \cdot (-3) \cdot (-4) \cdot (-5) \cdot 65! &\equiv -1 (\text{mod } 71) \\ 2 \cdot 3 \cdot 4 \cdot 5 \cdot 65! &\equiv 1 (\text{mod } 71) \\ 2 \cdot 36 \cdot 3 \cdot 24 \cdot 4 \cdot 18 \cdot 5 \cdot 14 \cdot 65! &\equiv 1 \cdot 36 \cdot 24 \cdot 18 \cdot 14 (\text{mod } 71) \\ -65! &\equiv 42 (\text{mod } 71) \\ 65! &\equiv 29 (\text{mod } 71) \end{aligned}$$

Logo, o resto é 29.

d)

$$\begin{aligned} 60! &\equiv -1 (\text{mod } 61) \\ 60 \cdot 59 \cdot 58 \cdot 57 \cdot 56 \cdot 55 \cdot 54 \cdot 53! &\equiv -1 (\text{mod } 61) \\ (-1) \cdot (-2) \cdot (-3) \cdot (-4) \cdot (-5) \cdot (-6) \cdot (-7) \cdot 53! &\equiv -1 (\text{mod } 61) \\ 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 53! &\equiv 1 (\text{mod } 61) \\ 5040 \cdot 53! &\equiv 1 (\text{mod } 61) \\ 38 \cdot 53! &\equiv 1 (\text{mod } 61) \\ 53 \cdot 38 \cdot 53! &\equiv 1 \cdot 53 (\text{mod } 61) \\ 53! &\equiv 53 (\text{mod } 61) \end{aligned}$$

Logo, o resto é 53.

e) $139 \mid 149! = 149 \cdot 148 \cdots 139 \cdots 2 \cdot 1$. Logo, o resto é 0.

Exercício 19.
Resolva

a) $\varphi(n) = n/3$.

b) $\varphi(2x) = \varphi(3x)$.

c) $\varphi(x) = 2$.

d) $\varphi(x) = 2x/3$.

e) $\varphi(x) = 6$.

Solução 19.

a) Seja $n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_k}^{\alpha_k}$

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$$\frac{n}{3} = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$$\frac{1}{3} = \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Como $\left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = \frac{1}{2} \cdot \frac{2}{3} = \frac{1}{3}$, os primos que compõem n são apenas 2 e 3. Assim, $n = 2^{\alpha_1}3^{\alpha_2}$, $\alpha_1, \alpha_2 \in \mathbb{N}$.

b) Seja $x = 2^{\alpha_1}3^{\alpha_2} \cdot y$ com $\text{mdc}(2, y) = \text{mdc}(3, y) = 1$. Assim, para $\alpha_1, \alpha_2 \geqslant 1$, temos:

$$\varphi(2x) = \varphi(2^{\alpha_1+1} \cdot 3^{\alpha_2} \cdot y) = \varphi(2^{\alpha_1+1})\varphi(3^{\alpha_2})\varphi(y) = 2^{\alpha_1} \cdot 2 \cdot 3^{\alpha_2-1}\varphi(y) = 2^{\alpha_1+1} \cdot 3^{\alpha_2-1}\varphi(y)$$

$$\varphi(3x) = \varphi(2^{\alpha_1} \cdot 3^{\alpha_2+1} \cdot y) = \varphi(2^{\alpha_1})\varphi(3^{\alpha_2+1})\varphi(y) = 2^{\alpha_1-1} \cdot 2 \cdot 3^{\alpha_2}\varphi(y) = 2^{\alpha_1} \cdot 3^{\alpha_2}\varphi(y)$$

Como $\varphi(2x) = \varphi(3x)$, temos:

$$2^{\alpha_1+1} \cdot 3^{\alpha_2-1}\varphi(y) = 2^{\alpha_1} \cdot 3^{\alpha_2}\varphi(y)$$

$$2^{\alpha_1+1} \cdot 3^{\alpha_2-1} = 2^{\alpha_1} \cdot 3^{\alpha_2} \Rightarrow 2 = 3,$$

o que é absurdo, logo $\alpha_1 = 0$ ou $\alpha_2 = 0$. No primeiro caso, não obtemos solução. Já no segundo caso, obtemos. Logo $x = 2^{\alpha_1} \cdot 3^0 \cdot 5^{\alpha_3} \cdots$, $\alpha_k \in \mathbb{N}$.

c) Seja $x = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_k}^{\alpha_k}$

$$\varphi(x) = \varphi\left({p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_k}^{\alpha_k}\right) = \left(p_1^{\alpha_1} - p_1^{\alpha_1-1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2-1}\right)\cdots\left(p_k^{\alpha_k} - p_k^{\alpha_k-1}\right)$$

$$2 = p_1^{\alpha_1-1} \cdot p_2^{\alpha_2-1} \cdots p_k^{\alpha_k-1} \cdot (p_1 - 1) \cdot (p_2 - 1) \cdot (p_k - 1).$$

Note que, como $p_i - 1 \mid 2$, então $p_i = 2$ ou $p_i = 3$. Logo, $x = 2^{\alpha_1}3^{\alpha_2}$.

Para $\alpha_1 = 0$, temos $\varphi(x) = \varphi\left(3^{\alpha_2}\right) = 2 \cdot 3^{\alpha_2-1} = 2 \Rightarrow \alpha_2 = 1 \Rightarrow x = 3$.

Para $\alpha_1 = 1$, temos $\varphi(x) = \varphi\left(2^1 3^{\alpha_2}\right) = 2 \cdot 3^{\alpha_2-1} = 2 \Rightarrow \alpha_2 = 1 \Rightarrow x = 2 \cdot 3 = 6$.

Para $\alpha_1 = 2$, temos $\varphi(x) = \varphi\left(2^2 3^{\alpha_2}\right) = 2 \cdot \varphi\left(3^{\alpha_2}\right) = 2 \Rightarrow \alpha_2 = 0 \Rightarrow x = 2^2 = 4$.

d) Seja $x = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$

$$\varphi(x) = x \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$$\frac{2x}{3} = x \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$$\frac{2}{3} = \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Como $1 - \frac{1}{3} = \frac{2}{3}$, o único primo que compõe n é 3. Assim, $n = 3^{\alpha_2}$, $\alpha_2 \in \mathbb{N}$.

e) Seja $x = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$

$$\varphi(x) = \varphi\left({p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}\right) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \cdots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right)$$

$$6 = p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k - 1} \cdot (p_1 - 1) \cdot (p_2 - 1) \cdot (p_k - 1).$$

Note que, como $p_i - 1 \mid 6$, então $p_i = 2$, $p_i = 3$ ou $p_i = 7$. Logo, $x = 2^{\alpha_1} 3^{\alpha_2} 7^{\alpha_3}$.

Para $\alpha_1 = 0$, temos $\varphi(x) = \varphi\left(3^{\alpha_2} 7^{\alpha_3}\right) = 6$. Se $\alpha_2 = 0$, então $\varphi\left(7^{\alpha_3}\right) = 6 \Rightarrow \alpha_3 = 1$ e $x = 7$; se $\alpha_3 = 0$, então $\varphi\left(3^{\alpha_2}\right) = 6 \Rightarrow \alpha_2 = 2$ e $x = 9$.

Para $\alpha_1 = 1$, temos $\varphi(x) = \varphi\left(2^1 3^{\alpha_2} 7^{\alpha_3}\right) = \varphi\left(3^{\alpha_2} 7^{\alpha_3}\right) = 6$, e obtemos os mesmos valores anteriores $\alpha_2 = 0$ e $\alpha_3 = 1$ ou $\alpha_2 = 2$ e $\alpha_3 = 0$, logo $x = 14$ ou $x = 18$.

Para $\alpha_1 = 2$, temos $\varphi(x) = \varphi\left(2^2 3^{\alpha_2} 7^{\alpha_3}\right) = 2 \cdot \varphi\left(3^{\alpha_2} 7^{\alpha_3}\right) = 6 \Rightarrow \varphi\left(3^{\alpha_2} 7^{\alpha_3}\right) = 3$, que não possui solução.

Exercício 20.
Mostre que para todo n temos

a) $\varphi(4n) = 2\varphi(2n)$;

b) $\varphi(4n + 2) = \varphi(2n + 1)$;

Solução 20.

a) Seja $n = 2^\alpha \cdot m$ com $\text{mdc}(2, m) = 1$. Assim, para $\alpha \geqslant 0$, temos:

$$\varphi(4n) = \varphi(2^2 \cdot 2^\alpha \cdot m) = \varphi(2^{\alpha+2} \cdot m) = \varphi(2^{\alpha+2})\varphi(m) = 2^{\alpha+1} \cdot \varphi(m).$$

Por outro lado

$$\varphi(2n) = \varphi(2^1 \cdot 2^\alpha \cdot m) = \varphi(2^{\alpha+1} \cdot m) = \varphi(2^{\alpha+1})\varphi(m) = 2^\alpha \cdot \varphi(m).$$

Logo, $\varphi(4n) = \varphi(2n)$.

b) Como $\varphi(4n + 2) = \varphi(2 \cdot (2n + 1))$ e $\text{mdc}(2, 2n + 1) = 1$, então $\varphi(2 \cdot (2n + 1)) = \varphi(2) \cdot \varphi(2n + 1) = \varphi(2n + 1)$.