Questão 1.

(1,0) (a) Descreva os números naturais que possuem 15 divisores naturais.

(1,0) (b) Determine o menor número natural com 15 divisores.

UMA SOLUÇÃO

Dado o número n cuja decomposição em fatores primos é $p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, o número de divisores naturais de n é dado pela fórmula $d(n) = (\alpha_1 + 1) \cdots (\alpha_r + 1)$.

(a) Se $d(n) = 15$, temos duas opções:

(i) $r = 1$ e $\alpha_1 + 1 = 15$, ou

(ii) $r = 2$, $\alpha_1 + 1 = 3$ e $\alpha_2 + 1 = 5$.

Portanto, temos duas possibilidades: $n = p^{14}$, ou $n = p^2 q^4$, com p e q primos distintos.

(b) Os candidatos a menor número natural com 15 divisores naturais são: 2^{14} e $3^2 2^4$, sendo o menor deles o número $3^2 2^4$.

Questão 2.

(2,0) Determine a maior potência de 15 que divide 150!

UMA SOLUÇÃO

Se $E_3(150!) = n$ e $E_5(150!) = m$, então o expoente da maior potência de 15 que divide 150! é $E_{15}(150!) = \min\{n, m\}$. Vamos determinar $E_3(150!)$ e $E_5(150!)$:

$150 = 50 \times 3 + 0$, $50 = 16 \times 3 + 2$, $16 = 5 \times 3 + 1$ e $5 = 1 \times 3 + 2$,

$150 = 30 \times 5 + 0$, $30 = 6 \times 5 + 0$, e $6 = 1 \times 5 + 1$.

Portanto, $E_3(150!) = 50 + 16 + 5 + 1 = 72$ e $E_5(150!) = 30 + 6 + 1 = 37$. Consequentemente, $E_{15}(150!) = 37$.

Questão 3.

(2,0) Quando um macaco sobe uma escada de dois em dois degraus, sobra um degrau, quando sobe de três em três degraus, sobram dois degraus e quando sobe de cinco em cinco degraus, sobram três degraus. Quantos degraus possui a escada, sabendo que o número de degraus está entre 150 e 200 ?

UMA SOLUÇÃO

O número x de degraus é solução do seguinte sistema de congruências:

$$\begin{cases} X \equiv 1 \bmod 2 \\ X \equiv 2 \bmod 3 \\ X \equiv 3 \bmod 5 \end{cases}$$

Com as notações do Teorema Chinês dos Restos, temos $N = 2 \times 3 \times 5 = 30$, $N_1 = 15$, $N_2 = 10$ e $N_3 = 6$. Seja $(y_1, y_2, y_3) = (1, 1, 1)$ solução do sistema

$$\begin{cases} 15Y_1 \equiv 1 \bmod 2 \\ 10Y_2 \equiv 1 \bmod 3 \\ 6Y_3 \equiv 1 \bmod 5. \end{cases}$$

Portanto, toda solução do sistema original é da forma

$$x \equiv N_1 y_1 1 + N_2 y_2 2 + N_3 y_3 3 \mod 30,$$

ou seja, $x \equiv 53 \mod 30$. Assim, a solução entre 150 e 200 é $53 + 120 = 173$.

Outra solução: Como $n \equiv 3 \bmod 5$ e n tem que ser ímpar, pois $n \equiv 1 \bmod 2$, ficamos apenas com as seguintes possibilidades: 153, 163, 173, 183, 193. Então excluímos os múltiplos de 3 (153 e 183) e os "múltiplos de 3 $+1$"(163 e 193). Sobra 173.

Questão 4.

(1,0) (a) Determine os elementos invertíveis de $\mathbb{Z}_{24}$ e mostre que cada um é o seu próprio inverso.

(0,5) (b) Calcule a soma de todos os elementos invertíveis de $\mathbb{Z}_{24}$.

(0,5) (c) Calcule o produto de todos os elementos invertíveis de $\mathbb{Z}_{24}$.

UMA SOLUÇÃO

(a) Os elementos invertíveis de $\mathbb{Z}_{24}$ são da forma $[a]$, onde $a < 24$ e tal que $(a, 24) = 1$. Portanto, esses são [1], [5], [7], [11], [13], [17], [19] e [23]. Agora,

$1^2 \equiv 1 \text{ mod } 24,\ \ 5^2 = 25 \equiv 1 \text{ mod } 24,\ \ 7^2 = 2 \times 24 + 1 \equiv 1 \text{ mod } 24,$

$11^2 = 5 \times 24 + 1 \equiv 1 \text{ mod } 24,\ \ 13^2 = 7 \times 24 + 1 \equiv 1 \text{ mod } 24,$

$17^2 = 12 \times 24 + 1 \equiv 1 \text{ mod } 24,\ \ 19^2 = 15 \times 24 + 1 \equiv 1 \text{ mod } 24,$

$23^2 = 22 \times 24 + 1 \equiv 1 \text{ mod } 24.$

Logo, $[a]^2 = 1$, para $a = 5, 7, 11, 13, 17, 19, 23$.

(b) Temos que

$$[1] + [5] + [7] + [11] + [13] + [17] + [19] + [23] = [96] = [4 \times 24] = [0].$$

(c) Por outro lado,

$$[1] \times [5] \times [7] \times [11] \times [13] \times [17] \times [19] \times [23] = 1,$$

pois $[5] \times [7] = [11]$, $[13] \times [17] = [5]$ e $[19] \times [23] = [5]$.

Outra Solução:

(a) Como $13 \equiv -11 \text{ mod } 24$, $17 \equiv -7 \text{ mod } 24$, $19 \equiv -5 \text{ mod } 24$ e $23 \equiv -1 \text{ mod } 24$, então basta verificar a afirmação em apenas metade dos números.

(b) Segue imediatamente da argumentação acima que soma é zero mod 24.

(c) Como o produto de dois inversos aditivos é $-[1]$, e são quatro pares de elementos mutuamente inversos aditivamente, o produto é $(-[1])(-[1])(-[1])(-[1]) = [1]$.

Questão 5.

(1,0) (a) Seja dado um número natural $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ decomposto em fatores irredutíveis. Seja n um número natural tal que $\varphi(p_i^{\alpha_i})$ divide n, para todo $i = 1, \dots, r$. Mostre que m divide $a^n - 1$ para todo número natural a primo com m.

(1,0) (b) Mostre que $a^{12} - 1$ é divisível por 4095 sempre que $(a, 1365) = 1$.

UMA SOLUÇÃO

(a) Como $(a, m) = 1$ implica $(a, p_i^{\alpha_i}) = 1$, então o Teorema de Euler garante que $a^{\varphi(p_i^{\alpha_i})} \equiv 1 \bmod p_i^{\alpha_i}$. Como $\varphi(p_i^{\alpha_i})$ divide n, então $a^n \equiv 1 \bmod p_i^{\alpha_i}$, para todo $i = 1, \dots, r$. Mas isso é o mesmo que dizer que $a^n - 1$ é múltiplo de $p_i^{\alpha_i}$, $\forall i = 1, \dots, r$. Como os $p_i^{\alpha_i}$ são todos primos entre si, $a^n - 1$ é múltiplo de $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$.

(b) Note que $4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$ e que $1365 = 3 \cdot 5 \cdot 7 \cdot 13$. Então $(a, 1365) = 1$ implica (de fato, equivale a) $(a, 4095) = 1$. Portanto queremos saber se $a^{12} - 1$ é múltiplo de 4095, sob a hipótese $(a, 4095) = 1$. Pelo item anterior (com $n = 12$ e $m = 4095$), é suficiente verificar se $\varphi(3^2)$, $\varphi(5)$, $\varphi(7)$ e $\varphi(13)$ são divisores de 12. De fato, eles são: $\varphi(3^2) = 6$, $\varphi(5) = 4$, $\varphi(7) = 6$ e $\varphi(13) = 12$.

Evidentemente é possível responder a parte (b) sem estar muito ciente de um resultado geral como a parte (a), essencialmente fazendo as mesmas coisas. Queremos que $a^{12} - 1$ seja múltiplo de 4095 e, para tanto, basta que seja simultaneamente múltiplo de 3^2, 5, 7 e 13, pois são primos entre si. Então queremos mostrar as congruências $a^{12} \equiv 1 \bmod 9$, $a^{12} \equiv 1 \bmod 5$, $a^{12} \equiv 1 \bmod 7$ e $a^{12} \equiv 1 \bmod 13$. A hipótese $(a, 1365) = 1$ garante que $(a, 9) = 1$, $(a, 5) = 1$, $(a, 7) = 1$ e $(a, 13) = 1$. Com isso o Teorema de Euler garante que $a^{\phi(9)} = a^6 \equiv 1 \bmod 9$, logo $a^{12} = (a^6)^2 \equiv 1 \bmod 9$. Para os demais casos o Teorema de Euler coincide com o Pequeno Teorema de Fermat: $a^4 \equiv 1 \bmod 5$ implica $a^{12} = (a^4)^3 \equiv 1 \bmod 5$; $a^6 \equiv 1 \bmod 7$ implica $a^{12} = (a^6)^2 \equiv 1 \bmod 7$; e $a^{12} \equiv 1 \bmod 13$ já é o que queríamos demonstrar.