Questão 1.

(1,5) Sejam a e b dois números naturais tais que $(a, b) = pq$, em que p e q são dois números primos distintos. Quais são os possíveis valores de

(a) (a^2, b)?

(b) (a^3, b)?

(c) (a^2, b^3)?

UMA SOLUÇÃO

Suponhamos que $a = p^r q^s c$ e $b = p^u q^v d$, onde c e d são primos entre si e também com p e q. A hipótese $(a, b) = pq$ implica que $\min\{r, u\} = 1$ e $\min\{s, v\} = 1$.

(a) $a^2 = p^{2r} q^{2s} c^2$, onde c^2 é primo com p, q e d. Logo, $(a^2, b) = p^{\min\{2r,u\}} q^{\min\{2s,v\}}$. Tanto $\min\{2r, u\}$ como $\min\{2s, v\}$ podem e só podem assumir os valores 1 e 2. Portanto, são possíveis $(a^2, b) = pq$, $(a^2, b) = p^2 q$, $(a^2, b) = pq^2$, ou $(a^2, b) = p^2 q^2$.

(b) $(a^3, b) = p^l q^t$, com $l = \min\{3r, u\}$ e $t = \min\{3s, v\}$. Logo, $l \in \{1, 2, 3\}$ e $t \in \{1, 2, 3\}$.

(c) $(a^2, b^3) = p^l q^t$, com $l \in \{2, 3\}$ e $t \in \{2, 3\}$.

Questão 2.

(2,0) Ache o resto da divisão por 17 do número

$$S = 1^{16} + 2^{16} + 3^{16} + \cdots + 85^{16}.$$

UMA SOLUÇÃO

Pelo Pequeno Teorema de Fermat temos que

$$a^{16} \equiv \begin{cases} 1, & \text{se 17 não divide } a \\ 0, & \text{se 17 divide } a \end{cases} \qquad \text{mod } 17$$

Como $85 = 17 \times 5$, temos que de 1 a 85 há 5 múltiplos de 17 e $85 - 5 = 80$ não múltiplos de 17 (i.e., primos com 17), logo

$$S \equiv 80 \times 1 \text{ mod } 17 \equiv 12 \text{ mod } 17.$$

Portanto, o resto da divisão de S por 17 é 12.

Questão 3.

(1,5) É possível repartir exatamente $\binom{2357}{528}$ objetos entre 49 pessoas?

UMA SOLUÇÃO

Temos

$$a = \binom{2357}{528} = \frac{2357!}{1829!528!}.$$

Portanto, o expoente da maior potência de 7 que divide a é dado por

$$E_7(2357!) - E_7(1829!) - E_7(528!).$$

Agora

$2357 = 7 \times 336 + 5$, $336 = 7 \times 48 + 0$, $48 = 7 \times 6 + 6$.

$1829 = 7 \times 261 + 2$, $261 = 7 \times 37 + 2$, $37 = 7 \times 5 + 2$.

$528 = 7 \times 75 + 3$, $75 = 7 \times 10 + 5$, $10 = 7 \times 1 + 3$.

Assim,

$E_7(2357!) = 336 + 48 + 6 = 390$,

$E_7(1829!) = 261 + 37 + 5 = 303$ e

$E_7(528!) = 75 + 10 + 1 = 86$.

Logo,

$E_7(2357!) - E_7(1829!) - E_7(528!) = 390 - 303 - 86 = 1$.

Portanto, $49 = 7^2$ não divide a e a resposta do problema é **não**.

Questão 4.

(2,0) Dispomos de uma quantia de x reais menor do que 3000. Se distribuirmos essa quantia entre 11 pessoas, sobra um real; se a distribuirmos entre 12 pessoas, sobram dois reais, e se a distribuirmos entre 13 pessoas, sobram 3 reais. De quantos reais dispomos?

Sugestão: Pode ser útil utilizar o seguinte fato: c é solução da congruência $ay \equiv b \bmod m$ se, e somente se, c é solução da congruência $ry \equiv b \bmod m$, onde r é o resto da divisão de a por m.

UMA SOLUÇÃO

O número x de Reais é uma solução do seguinte sistema de congruências:

$$\begin{cases} X \equiv 1 \bmod 11 \\ X \equiv 2 \bmod 12 \\ X \equiv 3 \bmod 13 \end{cases}$$

Com as notações do Teorema Chinês dos Restos, temos $N = 11 \times 12 \times 13 = 1716$, $N_1 = 12 \times 13 = 156$, $N_2 = 11 \times 13 = 143$ e $N_3 = 11 \times 12 = 132$. Precisamos determinar uma solução do sistema:

$$\begin{cases} N_1 Y_1 \equiv 1 \bmod 11 \\ N_2 Y_2 \equiv 1 \bmod 12 \\ N_3 Y_3 \equiv 1 \bmod 13 \end{cases}$$

Utilizando a sugestão, podemos resolver o sistema:

$$\begin{cases} 2Y_1 \equiv 1 \bmod 11 \\ 11Y_2 \equiv 1 \bmod 12 \\ 2Y_3 \equiv 1 \bmod 13 \end{cases}$$

que possui a solução $(y_1, y_2, y_3) = (6, 11, 7)$ (achada por inspeção). Assim, as soluções do sistema de congruências são da forma

$$x \equiv N_1 \times y_1 \times 1 + N_2 \times y_2 \times 2 + N_3 \times y_3 \times 3 = 156 \times 6 \times 1 + 143 \times 11 \times 2 + 132 \times 7 \times 3 = 6854 \bmod 1716.$$

A menor solução é dada pelo resto da divisão de 6854 por 1716 que é 1706. A próxima solução é $1706 + 1716 = 3422$, que ultrapassa 3000. Portanto, a solução procurada é 1706.

Outra solução. Usando-se números negativos pode-se perceber, por inspeção, que -10 é solução do sistema de congruências. Então basta somar $N = 1716$ para se obter a primeira solução positiva (igual a 1706) e a seguinte, que ultrapassa 3000.

Recomendação aos professores. No material da disciplina optou-se pelo estudo de congruências sem a utilização dos negativos. Pretende-se rever essa decisão para o ano que vem, visto que os negativos são úteis e perfeitamente naturais na abordagem deste assunto. De qualquer forma, a banca entende que esta solução também deve ser considerada correta.

Questão 5.

(1,0) Sabendo que $7^4 = 2401$, ache os algarismos da dezena e da unidade do número 7^{99999}.

UMA SOLUÇÃO

Efetivamente, precisamos encontrar o resto da divisão de 7^{99999} por 100.

Como $99999 = 4 \times 24444 + 3$ e $7^4 \equiv 1 \bmod 100$, temos que

$$(7^4)^{24444} \equiv 1 \bmod 100.$$

Assim,

$$7^{99999} = (7^4)^{24444} \times 7^3 \equiv 1 \times 7^3 \bmod 100 \equiv 43 \bmod 100.$$

Portanto, os algarismos são 4, da dezena, e 3, da unidade.

Questão 6.

Considere $\mathbb{Z}_m$ para $m > 2$.

(0,5) (a) Mostre que $\mathbb{Z}_m$ tem sempre um número par de elementos invertíveis. *Sugestão:* Analise a paridade de $\varphi(m)$, quando $m > 2$.

(0,5) (b) Mostre que se $[a]$ é invertível em $\mathbb{Z}_m$, então $-[a] = [m-a]$ é invertível e $[a] \neq -[a]$.

(0,5) (c) Mostre que a soma de todos os elementos invertíveis de $\mathbb{Z}_m$ é igual a 0.

(0,5) (d) Mostre que a soma de todos os elementos de um sistema reduzido qualquer de resíduos módulo m é sempre múltiplo de m.

Observação: em cada item, pode-se usar a afirmação cuja demonstração é pedida em um item anterior sem necessariamente tê-la demonstrado.

UMA SOLUÇÃO

(a) Se $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, então $\varphi(m) = p_1^{\alpha_1 - 1} \dots p_r^{\alpha_r - 1}(p_1 - 1) \dots (p_r - 1)$, que é obviamente par se $m > 2$. Como o número de elementos invertíveis de $\mathbb{Z}_m$ é $\varphi(m)$, o resultado segue.

(b) Se $[b]$ é um inverso de $[a]$, é imediato ver que $(-[a])(-[b]) = [a][b] = 1$, logo $-[a]$ é invertível.

Se $[a]$ é invertível, então $(a, m) = 1$. Suponhamos por absurdo que $[a] = -[a]$, logo $[2a] = 2[a] = [0]$, o que implica que $2a = tm$, para algum $t \in \mathbb{N}$. Como m divide $2a$ e $(m, a) = 1$, segue-se que m divide 2, o que implica que $m = 2$, absurdo.

(c) Os elementos invertíveis se apresentam aos pares, um simétrico do outro, a soma é portanto zero.

(d) Se $a_1, \dots, a_{\varphi(m)}$ é um sistema reduzido de resíduos módulo m, temos que $[a_1], \dots, [a_{\varphi(m)}]$ são os elementos invertíveis de $\mathbb{Z}_m$, logo

$$[a_1 + \dots + a_{\varphi(m)}] = [a_1] + \dots + [a_{\varphi(m)}] = [0],$$

o que implica que $a_1 + \dots + a_{\varphi(m)}$ é um múltiplo de m.