Questão 1 [2,0 pt]

Determine o resto da divisão do número $2222^{5555} + 5555^{2222}$ por 7.

Solução

(1) Sendo $2222 = 7 \cdot 317 + 3 \equiv 3 \bmod 7$, temos

$$2222^{5555} \equiv 3^{5555} \bmod 7.$$

Análogamente, $5555 = 7 \cdot 793 + 4 \equiv 4 \bmod 7$, donde

$$5555^{2222} \equiv 4^{2222} \bmod 7.$$

Obtemos assim, $2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} \bmod 7$.

(2) Como $(3,7) = (4,7) = 1$, usando o Pequeno Teorema de Fermat, temos $3^6 \equiv 1 \bmod 7$ e $4^6 \equiv\ 1 \bmod 7$. Escrevendo $5555 = 6 \cdot 925 + 5$ e $2222 = 6 \cdot 370 + 2$, segue que

$$3^{5555} + 4^{2222} = 3^{6 \cdot 925} \cdot 3^5 + 4^{6 \cdot 370} \cdot 4^2 \equiv 3^5 + 4^2 \bmod 7,$$

e assim,

$$2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} \equiv 3^5 + 4^2 \equiv 5 + 2 \equiv 0 \bmod 7.$$

Portanto, o resto da divisão de $2222^{5555} + 5555^{2222}$ por 7 é zero.

Questão 2 [2,0 pt]

Encontre a decomposição em fatores primos de 40! e determine com quantos zeros termina esse número.

Solução

Para resolvermos o problema, deveremos calcular $E_p(40!)$ para todo primo $p \leq 40$. Sendo $40 = 2.\underline{20} = 2.2.\underline{10} = 2.2.2.\underline{5} = 2.2.2.(2.\underline{2} + \underline{1})$, temos $E_2(40!) = 20 + 10 + 5 + 2 + 1 = 38$.

De modo análogo: $E_3(40!) = 13+4+1 = 18$, $E_5(40!) = 8+1 = 9$, $E_7(40!) = 5$, $E_{11}(40!) = 3$, $E_{13}(40!) = 3$, $E_{17}(40!) = 2$, $E_{19}(40!) = 2$, $E_{23}(40!) = E_{29}(40!) = E_{31}(40!) = E_{37}(40!) = 1$.

Portanto,

$$40! = 2^{38} \cdot 3^{18} \cdot 5^9 \cdot 7^5 \cdot 11^3 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23 \cdot 29 \cdot 31 \cdot 37.$$

Consequentemente, como há 9 fatores iguais a 5 e 38 fatores iguais a 2 na decomposição de 40! em fatores primos, concluimos que 40! termina com 9 zeros.

Questão 3 [2,0 pt]

Ao formar grupos de trabalho numa turma o professor verificou que, tomando grupos com 3 componentes sobrariam 2 alunos, com 4 componentes sobraria 1 aluno e que conseguiria formar grupos com 5 componentes, sem sobras, desde que ele próprio participasse de um dos grupos. Sabendo que a turma tem menos de 50 alunos, quais são as possíveis quantidades de alunos nessa turma?

Solução

Representamos por N o número de alunos da turma, onde $N \leq 50$. Sabemos que N é uma solução do seguinte sistema de congruências:

$$\begin{cases} x \equiv & 2 \mod 3 \\ x \equiv & 1 \mod 4 \\ x+1 \equiv & 0 \mod 5 \end{cases}$$

ou equivalentemente

$$\begin{cases} x \equiv & 2 \mod 3 \\ x \equiv & 1 \mod 4 \\ x \equiv & 4 \mod 5 \end{cases}.$$

Como $(3,4) = (3,5) = (4,5) = 1$ usaremos o Teorema Chinês dos Restos para resolvê-lo. Neste caso, $c_1 = 2, c_2 = 1$, $c_3 = 4$, $M = 3 \cdot 4 \cdot 5 = 60, M_1 = 20, M_2 = 15$ e $M_3 = 12$. Por outro lado, $y_1 = 2, y_2 = 3$ e $y_3 = 3$ são soluções, respectivamente, das congruências $20y_1 \equiv 1 \mod 3$, $15y_2 \equiv 1 \mod 4$ e $12y_3 \equiv 1 \mod 5$. Portanto,

$$x \equiv M_1y_1c_1 + M_2y_2c_2 + M_3y_3c_3 \mod 60.$$

Assim, $x \equiv 20 \cdot 2 \cdot 2 + 15 \cdot 3 \cdot 1 + 12 \cdot 3 \cdot 4 \equiv 29 \mod 60$. A solução geral do sistema é dada por $x = 29 + 60t$, onde $t \in \mathbb{Z}$, com uma única solução natural menor do que 50. Portanto, a quantidade de alunos na turma é exatamente 29.

Questão 4 [2,0 pt]

(a) Sejam a, k, m inteiros, com $m > 1$, e $(k, m) = 1$.
Se $a_1, \ldots, a_m$ é um sistema completo de resíduos módulo m, mostre que $a + ka_1, \ldots, a + ka_m$ também é um sistema completo de resíduos módulo m.

(b) Encontre um sistema completo de resíduos módulo 11 formado apenas por múltiplos de 6.

Solução

(a) Basta provar que $a + ka_1, \ldots, a + ka_m$ são, dois a dois, não congruentes módulo m. Suponhamos então que, $a + ka_i \equiv a + ka_j \mod m$, onde $1 \leq i, j \leq m$. Segue que $ka_i \equiv ka_j \mod m$ e como $(k, m) = 1$, $a_i \equiv a_j \mod m$. Agora, como $a_1, \ldots, a_m$ é um sistema completo de resíduos módulo m, concluimos que $i = j$.

(b) Considere o sistema completo de resíduos módulo 11: 0, 1, 2,..., 10. Como (6,11)=1, usando o item (a), concluimos que

$$6+6\cdot 0=6,\ 6+6\cdot 1=12,\ 6+6\cdot 2=18,\dots,6+6\cdot 10=66$$

também é um sistema completo de resíduos módulo 11. Portanto, obtemos um sistema completo de resíduos módulo 11 formado apenas por múltiplos de 6.

Questão 5 [2,0 pt]

Sejam p e q números primos distintos e $m = pq$. Considere α e β inteiros tais que $\alpha\beta \equiv 1 \bmod \varphi(m)$, onde $\varphi : \mathbb{N} \to \mathbb{N}$ é a função de Euler. Mostre que $x^{\alpha\beta} \equiv x \bmod m$, para todo inteiro x.

Sugestão: *Mostre que $x^{\alpha\beta} \equiv x \bmod p$ e $x^{\alpha\beta} \equiv x \bmod q$.*

Solução

Sendo $\alpha\beta \equiv 1 \bmod \varphi(m)$, escrevemos $\alpha\beta = 1 + k\varphi(m), k \in \mathbb{Z}$.

Como p e q números primos distintos, temos que $\varphi(m) = (p-1)\cdot(q-1)$.

Considere agora um inteiro qualquer x. Usando os dados, escrevemos

$$x^{\alpha\beta} = x^{1+k\varphi(m)} = x^{1+k(p-1)\cdot(q-1)} = x\cdot(x^{p-1})^{k(q-1)}.$$

(1) Se p divide x, então $x \equiv 0 \bmod p$, donde $x^{\alpha\beta} \equiv x \bmod p$.

(2) No caso, p não divide x, usando o Pequeno Teorema de Fermat, temos $x^{p-1} \equiv 1 \bmod p$, donde

$$x^{\alpha\beta} = x\cdot(x^{p-1})^{k(q-1)} \equiv x \bmod p.$$

Assim, para todo x inteiro, vale que $x^{\alpha\beta} = x \bmod p$ e, pela simetria, temos também que $x^{\alpha\beta} = x \bmod q$.
Finalmente, como p e q números primos distintos temos $x^{\alpha\beta} = x \bmod pq$, portanto

$$x^{\alpha\beta} = x \bmod m.$$