Congruência Modular, Paridade e Princípio da Casa dos Pombos

Luiza Lanza e Andressa Farias

Caro leitor,

O objetivo deste material é trazer tópicos de matemática mais avançados, quando tratamos da prova da OBMEP, que podem auxiliar na resolução de questões. Congruência Modular, Paridade e Princípio da Casa dos Pombos são assuntos que, de certa forma, estão conectados entre si, e que podem tornar as demonstrações mais curtas e elegantes, além de serem ferramentas necessárias para alguns problemas.

Dessa forma, este artigo está divido em três subtópicos, em que tratamos separadamente destes assuntos e, ao final, deixamos questões que abordam os três conteúdos. Bons estudos!

1 Congruência Modular

Definição 1. *Dizemos que $a \equiv b \ (mod\ m)$, para $a, b, c \in \mathbb{Z}$ se* $\boldsymbol{a}$ *e* $\boldsymbol{b}$ *deixam restos iguais na divisão por* $\boldsymbol{m}$*. Lê-se* $\boldsymbol{a}$ *é congruente a* $\boldsymbol{b}$ *módulo* $\boldsymbol{m}$*.*

Relembrando: divisão euclidiana

$$\begin{array}{r|l} n & q \\ \hline r & p \end{array} \Rightarrow p \cdot q + r = m$$

$\therefore$ n ≡ r (mod q)

Uma propriedade fundamental da divisão euclidiana é que só há uma possibilidade de quociente e resto para a divisão.

Para $n, p, q, r \in \mathbb{Z}$, tem-se que o quociente de n divido por p é q e a divisão deixa resto r. Dessa forma, pode-se dizer que $n \equiv r \ (mod\ p)$.

Da definição da divisão euclidiana, há duas conclusões. Em primeiro lugar, n pode ser escrito como $n = p \times q + r$. A segunda conclusão é que a condição de existência do resto r é $0 \leq \ r < |n|$, do contrário, se $r > |n|$, é possível dividir novamente o resto por n, resultando em um quociente $q + 1$ e um resto $r' < |n|$

Propriedades de Congruência Modular

Propriedade 1: $a \equiv b \ (mod\ m) \Leftrightarrow a - b$ é divisível por m.

Demonstração: a e b são congruentes entre si no módulo m, i.e., deixam restos iguais na divisão por m, ao qual chamaremos de r. Como vimos anteriormente, a e b podem ser escritos como $a = m \times q_1 + r$ e $b = m \times q_2 + r$.

Dizer que um número é divisível por outro é o mesmo que dizer que o primeiro deixa resto 0 na divisão pelo segundo. Logo, queremos provar que $a - b \equiv 0 \ (mod\ m)$. Porém, $a - b = m \times q_1 + r - (m \times q_2 + r) = m(q_1 - q_2) + \cancel{r} - \cancel{r}$. Logo, $a - b = m(q_1 - q_2)$. Dessa forma, $m(q_1 - q_2)$ é divisível por m; o quociente desta divisão é $q_1 - q_2$ e o resto 0. Logo, $a \equiv b \ (mod\ m) \ \Leftrightarrow \ a - b \ \equiv \ 0 \ (mod\ m)$. □

Propriedade 2: $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m) \Leftrightarrow a \pm c \equiv b \pm d \ (mod\ m)$.

Demonstração: Analogamente à demonstração da propriedade 1, seja q_1, q_2, q_3, q_4 respectivamente os quocientes da divisão de a, b, c, d por m. Da mesma forma, considere que como $a \equiv b \ (mod\ m)$, a e b deixam resto r_1 na divisão por m, enquanto c e d deixam resto r_2 na divisão por m tal que $c \equiv d \ (mod\ m)$.

Dessa forma, podemos escrever estes números em função dos quocientes e restos na divisão por m, tal que $a = q_1 \times m + r_1$, $b = q_2 \times m + r_1$, $c = q_3 \times m + r_2$ e $d = q_4 \times m + r_2$. Assim,

$$a \pm c = q_1 \times m + r_1 \pm q_3 \times m + r_2 = m(q_1 \pm q_3) + r_1 \pm r_2$$

$$b \pm d = q_2 \times m + r_1 \pm q_4 \times m + r_2 = m(q_2 \pm q_4) + r_1 \pm r_2$$

Como $m(q_1 \pm q_3)$ é divisível por m, $m(q_1 \pm q_3) + r_1 \pm r_2$ deixa resto $r_1 \pm r_2$ na divisão por m. Da mesma forma, $m(q_2 \pm q_4)$ é divisível por m, portanto $m(q_2 \pm q_4) + r_1 \pm r_2$ deixa resto $r_1 \pm r_2$ na divisão por m, respeitando os sinais. Logo, $a + c$ e $b + d$ deixam resto $r_1 + r_2$ na divisão por m, da mesma forma $a - c$ e $b - d$

deixam resto $r_1 - r_2$ na divisão por m.

Como os restos são iguais, estes números são congruentes entre si no módulo m ! Logo,

$$a \equiv b\ (mod\ m); c \equiv d\ (mod\ m) \Leftrightarrow a + c \equiv b + d\ (mod\ m); a - c \equiv b - d\ (mod\ m)$$

□

Perceba que estas propriedades são válidas pois, idependentemente do quociente das divisões de $a \pm c$ e $b \pm d$ por m, a congruência modular só se preocupa em mostrar que os restos das divisões desses números por m são iguais. Essas propriedades serão muito úteis na resolução de problemas, como veremos mais à frente, principalmente problemas envolvendo divisibilidade.

Propriedade 3: $a \equiv b\ (mod\ m) \Leftrightarrow a \pm k \equiv b \pm k\ (mod\ m)$, para $k \in \mathbb{Z}$

Demonstração: Analogamente à Propriedade 1: *"a e b são congruentes entre si no módulo m, i.e., deixam restos iguais na divisão por m, ao qual chamaremos de r. Como vimos anteriormente, a e b podem ser escritos como* $a = m \times q_1 + r$ *e* $b = m \times q_2 + r$*."*

Portanto, $a \pm k = m \times q_1 + r \pm k$ e $b \pm k = m \times q_2 + r \pm k$. Como $m \times q_1$ é divisível por m, o resto da divisão de $a \pm k = m \times q_1 + r \pm k$ por m é $r \pm k$. Analogamente, o resto da divisão de $b \pm k$ por m é $r \pm k$. Como os restos da divisão de a e b por m são iguais, a e b continuam sendo congruentes entre si ao somar-se ou subtrair-se um número inteiro k de ambos os lados da congruência. □

Propriedade 4: $a \equiv b\ (mod\ m) \Leftrightarrow a \pm m \times k \equiv b\ (mod\ m)$

Demonstração: Escrevendo $a \pm m \times k$ como $a = m \times q_1 + r \pm m \times k \Rightarrow a = m(q_1 \pm k) + r$. Como $m(q_1 \pm k)$ é divisível por m, o resto da divisão de $a = m(q_1 \pm k) + r$ por m continua sendo r. Logo, $a \pm m \times k \equiv b\ (mod\ m)$. □

Propriedade 5: $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m) \Leftrightarrow a \times c \equiv b \times d\ (mod\ m)$.

Analogamente à demonstração da propriedade 2:

"Seja q_1, q_2, q_3, q_4 respectivamente os quocientes da divisão de a, b, c, d por m. Da mesma forma, considere que como $a \equiv b \ (mod \ m)$, a e b deixam resto r_1 na divisão por m, enquanto c e d deixam resto r_2 na divisão por m tal que $c \equiv d \ (mod \ m)$."

Dessa forma, podemos escrever estes números em função dos quocientes e restos na divisão por m, tal que $a = q_1 \times m + r_1$, $b = q_2 \times m + r_1$, $c = q_3 \times m + r_2$ e $d = q_4 \times m + r_2$". Assim,

$$a \times c = (q_1 m + r_1) \times (q_3 m + r_2) = q_1 q_3 m^2 + q_1 m r_2 + q_3 m r_1 + r_1 r_2$$

$$a \times c = m(q_1 q_3 m + q_1 r_2 + q_3 r_1) + r_1 r_2$$

Portanto, o resto da divisão de $a \times c$ por m é o produto de seus módulos na divisão por m, i.e., $r_1 r_2$. Analogamente, o resto de $b \times d$ na divisão por m é $r_1 r_2$. Logo, como os restos de $a \times c$ e $b \times d$ por m são iguais, $a \times c \equiv b \times d \ (mod \ m)$. □

Propriedade 6: $a \equiv b \ (mod \ m) \Leftrightarrow a^n \equiv b^n \ (mod \ m)$

Demonstração: Escrevemos a e b como $a = m \times q_1 + r$ e $b = m \times q_2 + r$. Dessa forma, $a^n = (m \times q_1 + r)^n = (m \times q_1 + r)(m \times q_1 + r)...(m \times q_1 + r) = (m \times q_1)^n + (m \times q_1)^{n-1} \times r + (m \times q_1)^{n-2} \times r^2 + ... + (m \times q_1)^{n-(n-1)} \times r^{n-1} + r^n$
Todas as parcelas da soma possuem o fator m, sendo divisíveis por m, com exceção do termo r^n. Logo, o resto da divisão de a^n por m é igual ao módulo da divisão de a por m também elevado à n-ésima potência, i.e., r^n. Analogamente, o resto da divisão de b^n por m tal que $b = m \times q_2 + r$ é r^n.

Logo, como a^n e b^n deixam restos iguais na divisão por m, dizemos que:

$$a^n \equiv b^n \ (mod \ m)$$

□

2 Princípio da Casa dos Pombos

O princípio da casa dos pombos, também conhecido como Princípio de Dirichlet, é razoavelmente simples, porém sua aplicação pode ser feita em problemas bem sofisticados!

Definição 2. *Se há n+1 pombos que devem entrar em n casas, é fato que há mais de um pombo em pelo menos uma casa.*

O primeiro passo para responder uma questão que utiliza esse princípio é identificar quando é um problema que o utiliza. Na maioria dos casos, as questões seguem o seguinte estilo:

Prove que em qualquer conjunto de n objetos, podemos escolher x deles tal que satisfazem a propriedade y.

Após a identificação, as perguntas a seguir norteiam a resolução de problemas por meio do Princípio da Casa dos Pombos:

- Quem e quantos são os pombos?
- Quem e quantas são as casas?

Por fim, basta distribuir os pombos nas casas e determinar a relação existente entre ambos.

Exemplos de aplicações básicas do princípio da casa dos pombos:

- Em um grupo de 13 pessoas, há pelo menos 2 que fazem aniversário no mesmo mês.
- Se temos 7 livros para alocar em 6 prateleiras de uma estante, pelo menos dois desses livros ficarão na mesma prateleira.
- Se 367 pessoas estão em um auditório, é garantido que pelo menos duas delas fazem aniversário no mesmo dia.
- Em uma sala de aula, há 27 pessoas, portanto, ao menos duas delas possuem os nomes começados com a mesma letra.
- Ao escolher 3 números, ao menos 2 deles possuem a mesma paridade.

PROBLEMAS RESOLVIDOS

Problema 1.(Putnam). São escolhidos 5 pontos em uma esfera. Mostre que existe um hemisfério (uma metade da esfera, obtida "cortando" a esfera ao meio em alguma direção) que contém pelo menos 4 dos pontos escolhidos. Obs.: Para os propósitos deste problema, os pontos que estão na borda dos hemisférios (os pontos que estão sobre a linha pela qual a esfera foi "cortada") pertencem a ambos os hemisférios.

Solução:

Dos cinco pontos, escolhemos dois e dividimos a esfera em dois hemisférios através de uma linha que passa por eles. Pelo princípio da casa dos pombos, ao menos dois dos três demais pontos pertencem ao mesmo hemisfério. Como os dois pontos que escolhemos inicialmente pertencem a ambos os hemisférios (pois estão sobre o corte), há ao menos quatro pontos no mesmo hemisfério.

Problema 2.(POTI N2-adaptado)
a) Dados 7 inteiros positivos, prove que existem dois cuja soma ou diferença é um múltiplo de 10.

Solução:

Queremos provar que $a + b \equiv 0 \ (mod\ 10)$ ou $a - b \equiv 0 \ (mod\ 10)$. O resultado da soma ou da subtração de dois números é múltiplo de 10 $\iff$ um deles ao ser dividido por 10 tenha um resto simétrico ao outro (ou a deixa o mesmo resto que b na divisão por 10 ou o resto que a deixa somado ao resto que b deixa é um múltiplo de 10), ou seja, $a \equiv \pm b \ (mod\ 10)$.

Para que a condição descrita pelo enunciado não seja aceita, não podem haver 2 números com o mesmo resto ao serem divididos por 10 e não podem haver 2 números que satisfaçam alguma das combinações a seguir (considere que os algarismos abaixo representam os restos deixados por 2 números na divisão por 10).

(9,1);(8,2);(7,3);(6,4);(5,5);(0,0) $\longrightarrow$ Perceba que os restos somados, dão um múltiplo de 10. Agora utilizamos o princípio da casa dos pombos, queremos escolher números que não estam no mesmo conjunto, pegando 1 número de cada conjunto acima totalizamos 6, porém são 7 números inteiros positivos, logo, no mínimo dois deles estará no mesmo conjunto.

b) Prove que qualquer conjunto de 10 inteiros possui algum subconjunto não vazio cuja soma dos elementos é um múltiplo de 10.

Solução:

Os subconjuntos possíveis podem ter 1 elemento, 2 elementos, 3 elementos, ... , ou 10 elementos. Portanto, podemos fazer somas com 1 elemento, 2 elementos, ..., 10 elementos.

$S_1 = a_1$

$S_2 = a_1 + a_2$

$\vdots$

$S_{10} = a_1 + a_2 + a_3 + ... + a_{10}$

Se houver uma dessas somas com resto 0 na divisão por 10, então o que é proposto no enunciado já é satisfeito, mas suponha que nenhuma dessas somas dê resto 0 na divisão por 10, logo, há 9 restos possíveis. Utilizando o Princípio da casa dos pombos, há 9 restos e 10 somas, logo, pelo menos duas somas deixam o mesmo resto ao serem divididas por 10.

Sem perda de generalidade, digamos que S_3 e S_5 possuem o mesmo resto ao serem divididos por 10.

$$\begin{cases} S_3 = \underline{a_1 + a_2 + a_3} \\ S_5 = \underline{a_1 + a_2 + a_3} + a_4 + a_5 \end{cases}$$

Logo, $a_4 + a_5$ é múltiplo de 10.

Problema 3. Uma caixa contém 10 bolas verdes, 10 bolas amarelas, 10 bolas azuis e 10 bolas vermelhas. Joãozinho quer retirar uma certa quantidade de bolas dessa caixa, sem olhar, para ter a certeza de que, entre elas, haja um grupo de 7 bolas com 3 cores diferentes, sendo três bolas de uma cor, duas bolas de uma segunda cor e duas bolas de uma terceira cor. Qual é o número mínimo de bolas que Joãozinho deve retirar da caixa?

Solução:

O número de bolas que Joãozinho pode retirar de forma que retire no máximo duas cores é $2 \times 10 = 20$. Pelo Princípio da Casa dos Pombos, Joãozinho precisa retirar no mínimo 20+1= 21 bolas para garantir que retirou bolas de 3 cores distintas. Porém, queremos garantir que há pelo menos 2 bolas de uma terceira cor. Logo, dentre os outros dois conjuntos de cores, o número mínimo de bolas que Joâozinho deve retirar para ter 2 bolas de uma terceira cor é 20+2+1= 23 bolas.

Problema 4.(OBMEP 2017) Joana retira bolas, sem reposição, de uma caixa com 2017 bolas numeradas de 1 a 2017.

a) Qual é a quantidade mínima de bolas que ela deve retirar para garantir que em pelo menos uma delas haja um número múltiplo de 3?

b) Qual é a quantidade mínima de bolas que ela deve retirar para garantir que existam duas bolas com a soma de seus números igual a um múltiplo de 3?

c) Qual é a quantidade mínima de bolas que ela deve retirar para garantir que existam duas bolas de modo que a soma de seus números seja um múltiplo de 3 e sua diferença seja um múltiplo de 2?

Solução:

a) Como $2017 = 672 \times 3 + 1$, sabemos que existem 672 números múltiplos de 3 de 1 à 2017. Logo, 1345 não são múltiplos de 3. Pelo Princípio da Casa dos Pombos, o número mínimo de bolas a ser retirado é todos os não-múliplos de 3 mais uma, logo ela precisa retirar 1345+1 = 1346 bolas.

b) O máximo de bolas múltiplas de 3 que Joana pode retirar para que isso não aconteça é uma, pois se duas bolas possuem números múltiplos de 3 a proposição já é atendida. Pensando nos números não-múltiplos de 3, estes podem ser congruentes a 1 ou 2 módulo 3. Se ela retira duas bolas de números a e b tal que $a \equiv 1\ (mod\ 3)$ e $b \equiv 2\ (mod\ 3) \Rightarrow a+b \equiv 0\ (mod\ 3)$. Como há 673 bolas com números congruentes a 1 módulo 3 e 672 bolas com números congruentes a 2 módulo 3, o número máximo de bolas que Joana pode tirar para que a soma de dois deles não seja múltiplo de 3 é 673+1= 674. Logo, pelo Princípio da Casa dos Pombos, o número mínimo de bolinhas que Joana precisa retirar para que isso ocorra é 674 **+1**= 675 bolas.

c) Sejam a e b dois números que atendem essas proposições. Como $a - b \equiv 0\ (mod\ 2)$, isso implica que a e b possuem a mesma paridade. Sendo A={3,6,9,...,2016} o conjunto de todos os mútiplos de 3 de 1 a 2017, o máximo de bolas que ela pode retirar desse conjunto de forma que a diferença de seus números não seja múltipla de 2 é duas bolas, de paridades opostas.

Sendo B={1,4,7,...2017} o conjunto dos números congruentes a 1 módulo 3 de 1 a 2017 e C={2,5,8,...,2015} o conjunto dos números congruentes a 2 módulo 3 de 1 a 2017, como mostrado no item b), para que a soma dos números de duas bolas seja divisível por 3 um deles deve pertencer ao conjunto B e um ao conjunto C. O conjunto B tem 673 elementos, sendo 336 pares e 337 ímpares, e o conjunto C tem 672 elementos, sendo 336 pares e 336 ímpares. Como os números devem ter a mesma paridade para que sua diferença seja divisível por 2, sendo um do conjunto B e um do C, o número máximo de bolas com números não-múltiplos de 3 que Joana pode retirar para que isso não aconteça é 336+337=673 bolas.

Logo, pelo Princípio da Casa dos Pombos, o número mínimo de bolas que ela deve retirar é 673+2**+1** = 676.

3 Paridade

Nesta seção, nos dedicaremos a estudar a paridade dos número e suas propriedades nas operações. Para demonstrar as propriedades de paridade, vamos retomar várias vezes as propriedades de congruência modular, demonstradas na primeira seção deste artigo.

Definição 3. *Um número é par se, ao ser divido por 2, resulta em um número inteiro. Todo número inteiro ou é par ou é ímpar.*

Disso, conclui-se que para P par, $P \equiv 0 \ (mod\ 2)$. Números pares também podem ser ditos aqueles que terminam em 0, 2, 4, 6 ou 8, pois este é o critério de divisibilidade por 2.

Sendo P par, P é divisível por 2, portanto é da forma $P = 2k$
$k \in \mathbb{Z}$.

3.1. Propriedades de Paridade

Propriedade 1: Dado um número n, a paridade do antecessor e sucessor de n é oposta à paridade de n

Em outras palavras, queremos provar que se n é par, $n-1$ e $n+1$ são ímpares, e se n é ímpar, $n-1$ e $n+1$ são pares.

Demonstração: Por congruência modular: se n é ímpar, $n \equiv 1 \ (mod\ 2)$. Logo, $n+1 \equiv 1+1 \ (mod\ 2) \Rightarrow n \equiv 2-2 \ (mod\ 2) \Rightarrow n \equiv 0 \ (mod\ 2)$. Da mesma forma, $n-1 \equiv 1-1 \ (mod\ 2) \Rightarrow n \equiv 0 \ (mod\ 2)$.

Se n é par, $n \equiv 0 \ (mod\ 2)$. Logo, $n+1 \equiv 0+1 \ (mod\ 2) \Rightarrow n \equiv 1 \ (mod\ 2)$. Da mesma forma, $n-1 \equiv 0-1 \ (mod\ 2) \Rightarrow n \equiv -1+2 \ (mod\ 2) \Rightarrow n \equiv 1 \ (mod\ 2)$. □

Ideias: tente demonstrar estas propriedades pela definição de paridade, ou seja, um número par é divisível por 2, portanto pode ser escrito na forma $2k$.

Propriedade 2: A soma ou subtração de dois números de mesma paridade resulta em um número par.

Demonstração: Se a e b têm a mesma paridade, então $a \equiv b \ (mod\ 2) \Rightarrow a - b \equiv 0 \ (mod\ 2)$, como demonstrado na Propriedade 1 da seção de Congruência Modular. Como $a - b$ é divisível por 2, $a - b$ é par.

Por outro lado, se $a \equiv b \ (mod\ 2)$, podemos somar b dos dois lados da congruência, conforme a Propriedade 3. Dessa forma, $a + b \equiv 2b \ (mod\ 2)$. Perceba que como $2b$ é par, $2b \equiv 0 \ (mod\ 2) \Rightarrow a + b \equiv 0 \ (mod\ 2)$. □

Propriedade 3: A soma ou subtração de dois números de paridades diferentes resulta em um número ímpar.

Demonstração: Seja a um número par e b um número ímpar.

$$\therefore a \equiv 0 \ (mod\ 2); b \equiv 1 \ (mod\ 2) \Rightarrow a + b \equiv 0 + 1 \ (mod\ 2) \Rightarrow a + b \equiv 1 \ (mod\ 2)$$

$$a - b \equiv 0 - 1 \mathbf{+2} \ (mod\ 2) \Rightarrow a - b \equiv 1 \ (mod\ 2)$$

□

Propriedade 4: O produto de um número par por outro número de qualquer paridade resulta em um número par.

Seja a um número par e b um número par ou ímpar. Dessa forma, $a \equiv 0 \ (mod\ 2)$ e, como não vamos assumir a paridade de b, dizemos que $b \equiv r \ (mod\ 2)$. Pela Propriedade 5 da seção de Congruência Modular, tem-se que $a \times b \equiv 0 \times r \ (mod\ 2) \Rightarrow a \times b \equiv 0 \ (mod\ 2)$. □

Propriedade 5: O produto de dois números ímpar resulta em um número ímpar.

Sejam a e b números ímpares, então $a \equiv 1 \ (mod\ 2)$ e $b \equiv 1 \ (mod\ 2)$. Pela Propriedade 5 de Congruência Modular, tem-se que $a \times b \equiv 1 \times 1 \ (mod\ 2) \Rightarrow a \times b \equiv 1 \ (mod\ 2)$. □

4 Exercícios resolvidos:

Questão 1 (Círculos Matemáticos: A Experiência Russa): Prove que $2222^{5555} + 5555^{2222}$ é divisível por 7.

Pela divisão euclidiana, sabemos que $2222 = 317 \times 7 + 3 \Rightarrow 2222 \equiv 3\ (mod\ 7)$. Elevando os dois lados ao cubo, temos que $2222^3 \equiv 3^3\ (mod\ 7) \Rightarrow 2222^3 \equiv 27\ (mod\ 3)$. Subtraindo $4 \times [módulo]$ de 27, temos $2222^3 \equiv -1\ (mod\ 7)$. Dividindo 5555/3, descobrimos maior número pelo qual conseguimos elevar 2222^3 para que o número seja menor ou igual a 2222^{5555} é 1851.

$$\therefore (2222^3)^{1851} \equiv (-1)^{1851}\ (mod\ 7)$$

$$\Rightarrow 2222^{5553} \equiv -1\ (mod\ 7)$$

Como $2222^2 \equiv 3^2$**-7** $(mod\ 7) \Rightarrow 2222^2 \equiv 2(mod\ 7)$ Logo, $2222^{5553} \times 2222^2 \equiv (-1) \times 2\ (mod\ 7) \Rightarrow 2222^{5555} \equiv -2\ (mod\ 7)$

$5555 = 793 \times 7 + 4 \Rightarrow 5555 \equiv 4\ (mod\ 7)$. Elevando os dois lados da congruência ao cubo, temos $5555^3 \equiv 4^3 - 9 \times 7\ (mod\ 7) \Rightarrow 5555^3 \equiv 1\ (mod\ 7)$. Analogamente ao que foi feito anteriormente, vamos elevar os dois lados à 740, assim temos que $(5555^3)^{740} \equiv 1^{740}\ (mod\ 7) \Rightarrow 5555^{2220} \equiv 1\ (mod\ 7)$. Como $5555^2 \equiv 4^2 - 2 \times 7\ (mod\ 7) \Rightarrow 5555^{2220} \times 5555^2 \equiv 1 \times 2\ (mod\ 7)$, $\therefore 5555^{2222} \equiv 2\ (mod\ 7)$. Logo, $2222^{5555} + 5555^{2222} \equiv -2 + 2\ (mod\ 7)$

$$\therefore 2222^{5555} + 5555^{2222} \equiv 0\ (mod\ 7)$$

□

Questão 2 (OMU 2023):

Questão 2:

1. Sejam $a > b > c$ números naturais. Seja P_3 o produto das diferenças (não negativas) entre estes números, ou seja, $P_3 = (a-b)(a-c)(b-c)$. Mostre que P_3 é par.

2. Sejam $a > b > c > d$ números naturais. Seja P_4 o produto das diferenças (não negativas) entre estes números, ou seja, $P_4 = (a-b)(a-c)(a-d)(b-c)(b-d)(c-d)$. Mostre que P_4 é múltiplo de 3.

3. Vamos agora considerar n números naturais $a_1 > a_2 > \cdots > a_n$ e seja

$$P_n := \prod_{1 \leqslant i < j \leqslant n} (a_i - a_j)$$

o produto de todas as diferenças não negativas entre estes números. Mostre que todo número $k < n$ é divisor de P_n.

1. Como há 3 números, e na divisão por 2 só há duas possibilidades de resto ($r \leq 2 / r \in \mathbb{Z} \Rightarrow r = (0, 1)$), pelo Princípio da Casa dos Pombos temos que pelo menos dois números deixam resto iguais na divisão por dois, ou seja, são congruentes entre si no módulo 2. Pela propriedade 1, temos que se $p \equiv q \ (mod\ 3) \Rightarrow p - q \equiv 0 \ (mod\ m)$. Portanto, ao menos uma das 3 diferenças é congruente a 0 módulo 2. Chamemos os restos das outras diferenças na divisão por 2 de r_1 e r_2. Logo,

$$(a-b)(a-c)(b-c) \equiv r_1 \times r_2 \times 0 \ (mod\ 2) \Rightarrow (a-b)(a-c)(b-c) \equiv 0 \ (mod\ 2)$$

. Como $(a-b)(a-c)(b-c)$ é divisível por 2, por definição, este número é par. □

2. Analogamente ao item 1, temos 4 números e 3 possibilidades de resto na divisão por 3, então pelo Princípio da Casa dos Pombos dois números são congruentes entre si no módulo 3, portanto sua diferença é congruente a 0 no módulo 3. Chamemos os restos das outras diferenças na divisão por 3 de r_1, r_2, r_3, r_4 e r_5. Logo,

$$(a-b)(a-c)(a-d)(b-c)(b-d)(c-d) \equiv r_1 \times r_2 \times r_3 \times r_4 \times r_5 \times 0 \ (mod\ 3)$$

$$\Rightarrow (a-b)(a-c)(a-d)(b-c)(b-d)(c-d) \equiv 0 \ (mod\ 3)$$

Como $(a-b)(a-c)(a-d)(b-c)(b-d)(c-d)$ é divisível por 3, ou seja, pode ser escrito como $3k$, este número é múltiplo de 3. □

3. Este item é uma generalização dos anteriores. Temos n números inteiros, sendo k inteiro tal que $k < n$, há k possibilidades de restos na divisão por k. Pelo Princípio da Casa dos Pombos, dentre n números, pelo menos dois são congruentes

entre si no módulo k. Logo, dizemos que estes dois números são congruentes a 0 no módulo k, e chamaremos os outros $\frac{n(n-1)}{2!}$ restos das outras diferenças na divisão por k de r_1, r_2, r_3,..., r_m. Logo,

$$\prod_{1\leq i\leq j\leq n}(a_i - a_j) \equiv r_1 \times r_2 \times r_3 \times ... \times 0 \ (mod\ k)$$

$$\prod_{1\leq i\leq j\leq n}(a_i - a_j) \equiv 0 \ (mod\ k)$$

□

Questão 3: Prova que $\sqrt{2}$ é irracional.

Suponha-se, por absurdo, que $\sqrt{2}$ é racional. Então, podemos escrever $\sqrt{2}$ como $\sqrt{2} = \frac{p}{q} / \ p,q \in \mathbb{Z};\ p \nmid q$ (p não divide q). Elevando os dois lados da igualdade ao quadrado, temos que $2 = \frac{p^2}{q^2} \Rightarrow 2q^2 = p^2$ (I). Portanto, concluímos que p^2 é par, e pelas propriedades de paridade sabemos que p também é par, porque se p fosse ímpar p^2 seria ímpar ($P \times P = P$, $I \times I = I$).

Como p é par, podemos escrever p na forma $p = 2k$, $\therefore p^2 = (2k)^2 \Rightarrow p^2 = 4k^2$ (II). Logo, (I)=(II)$\Rightarrow 2q^2 = 4k^2 \Rightarrow q^2 = 2k^2$. Concluímos então que q^2 é par e, portanto, q é par.

Como p e q são pares, eles têm o fator 2 em comum, logo p divide q, o que é um absurdo pela nossa hipótese inicial. Logo, $\sqrt{2}$ é irracional. □