D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA ~~OU REFUTAÇÃO~~.

PROVA

Pela def. 2 tem-se que se $a \equiv b \pmod{n}$, $n \mid a-b$, no entanto se temos um $k \in \mathbb{Z}$ t.q. $n.k \mid a-b$, então $a \equiv b$ (mod ~~7n~~ $k.n$). X

por que?

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
~~PROVA OU~~ REFUTAÇÃO.

REFUTAÇÃO

Se $a \equiv b \pmod{42}$, ~~=~~ $42 \mid a-b$ e se

?

?

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA ~~OU REFUTAÇÃO~~.

PROVA

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO. → QUAL O POSICIONAMENTO? ← Realmente

$m | (a-b) \rightarrow m \cdot q = (a-b)$

$m | 7(a-b) \rightarrow m \cdot q = 7(a-b) \rightarrow m \cdot \frac{q}{7} = (a-b)$?

$\cancel{q \frac{1}{7} \in \mathbb{Z}}$, ~~Provado~~ Qual a argumentação?

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

$42 | (a-b) \rightarrow 42 | 42a - 1 \rightarrow \frac{42}{42}$, REFUTADO

? ?? ✓ !!

O que é isso?

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
Prova ou Refutação.

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
Prova ou Refutação.

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
Prova ou Refutação.

1. $a \equiv b \pmod{n} \Rightarrow n \mid a-b \Rightarrow n.k_1 = a-b,\ k_1 \in \mathbb{Z}$
2. $b \equiv c \pmod{n} \Rightarrow n \mid b-c \Rightarrow n.k_2 = b-c,\ k_2 \in \mathbb{Z}$

1. $-b = n.k_1 - a \Rightarrow b = a - n.k_1$
Substituindo em 2.

2. $n.k_2 = a - n.k_1 - c$

Começou bem!
... faltou pouco para concluir!

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

~~Suponha que a = 5,~~
Considere que $a = 5$, $b = 2$ e $n = 3$. Pela definição é ~~possível concluir que~~ $5 \equiv 2 \pmod{3}$ se, e somente se, $3 \mid 5-2$, o que por sua vez é verdade, porém, $5 \equiv 2 \pmod{7 \cdot 3} \Leftrightarrow 21 \mid 5-2$, o que não é verdade.

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

ideia correta, cuidado na escrita

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
Prova ou Refutação.

Sejam $a = 5$, $b = 2$ e $n = 3$
$5 \equiv 2 \pmod{3}$
? $3 \mid 5 - 2$
? $7 \, 5 \equiv 2 \pmod{7 \cdot 3}$
? $21 \nmid 5 - 2$

idéia correta
cuidado na escrita.

✓

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
Prova ou Refutação.

Por definição de mod o b sempre será o resto da divisão de a por nesse caso 42.
então $42 \mid a - b$.

onde é isso na definição???

o que isso tem a ver com o que queremos provar/refutar?

✗

Prova ou refute $a \leq 42$ e $b \leq 42$

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
Prova ou Refutação.

i) $a \equiv b \pmod{n}$
? $n \mid a - b$
? $\exists q_1 \in \mathbb{Z} \therefore n q_1 = a - b$
ii) $b \equiv c \pmod{n}$
? $n \mid b - c$
? $\exists q_2 \in \mathbb{Z} \therefore n \cdot q_2 = b - c$
? $n \cdot q_1 = a - b$
? $n \cdot q_1 = a - (n q_2 + c)$
? $n \cdot (q_1 + q_2) = a - c$
? $n \cdot (-(q_1 + q_2)) = c - a \Rightarrow c \equiv a \pmod{n}$

✓

ideia correta
mas parece rascunho.

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

A AFIRMAÇÃO NÃO É VERDADEIRA ~~POIS PARA CONTRAPOSIÇÃO~~ O CASO ABAIXO A AFIRMAÇÃO NÃO É VERDADEIRA. contraexemplo

$6 \equiv 4 \pmod{2}$

isso é o que? (ideia correta!)

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

?

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

???

$a \equiv b \pmod{n} \Rightarrow n \mid a-b \Rightarrow n \cdot P = a-b$ (I)

$b \equiv c \pmod{n} \Rightarrow n \mid b-c \Rightarrow n \cdot Q = b-c$ (II)

SUBTRAINDO (I) DE (II)

$2n \cdot P \cdot Q = a-c$

$n(2 \cdot P \cdot Q) = a-c$

DESSA FORMA A AFIRMAÇÃO $c \equiv a \pmod{n}$ É VERDADEIRA.

??? como?

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

Contra exemplo
$a = 6, b = 3, n = 3$

? $6 \equiv 3 \pmod{3}$
?: $6 \not\equiv 3 \pmod{21}$

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

Para $n = 2$, $a = 5$ e $b = 1$:

$2 | 5 - 1$ ✓

$7 \cdot 2 | 5 - 1$ ✗

cuidado na escrita (parece rascunho).

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

Para $a = 168$ e $b = 84$ $\rightarrow$ $42 | 168 - 84$

? $42 | 84$ ✓

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

$n | a - b \rightarrow n \cdot q1 = a - \cancel{b}$

$n | b - c \rightarrow n \cdot q2 = \cancel{b} - c$ +

??

$n | c - a \rightarrow n \cdot q^3 = c - a$?

$n \cdot q1 + n \cdot q2 = a - c$

nem parecem subscripts

$n \cdot (q1 + q2) = a - c$

sendo $q1$ e $q2 \in \mathbb{Z}$ ✓

idéia correta.

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

Caso $a = 10$, $b = 16$ e $n = 3$ temos (REFUTAÇÃO)
$10 \equiv 16 \pmod{3} \not\equiv 10 \equiv 16 \pmod{21}$. perfeito.
Cuidado ao escolher números quaisquer
nenhum problema! Não são "quais quer". São bem escolhidos para servir como contraexemplo.

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

Caso $a = 86$, $b = 128$ temos que $86 \equiv 128 \pmod{42}$
(ambos são maiores que 42). Perfeito.
(REFUTAÇÃO) Obs. poderia tomar $a := 86$ e $b := 86$ também.

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

cuidado: o que é esse r?

Caso $a \equiv b \pmod{n} \rightarrow b = n.q_1 + r$
$\rightarrow a = n.q_2 + r$

$\rightarrow n \mid a - b$
$\exists q \in \mathbb{Z} : n \cdot q = a - b$

Como $c \equiv b \pmod{n} \rightarrow c = n.q_3 + r$

~~Pelo~~
Pelo definição: $c \equiv b \pmod{n}$, Pois deixam os mesmos restos feito divisão com um inteiro n.

Qual definição? ← Pois é.
Não pro usado que deixa o mesmo resto.

Idéia 100% correta (cuidado na escrita) mas presuponha outra definição de $- \equiv - (\mathrm{mod} -)$

D aqui sim,

cuidado!

por que o mesmo inteiro?

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

Se $a \equiv b \pmod{n}$, existe um inteiro K tal que $a - b = nK$, Então, para ~~$(a \equiv b (7n))$~~ $a \equiv b \pmod{7n}$ ~~...~~ teríamos $a - b = 7nK$. Mas sabemos que $\underbrace{nK \mid a-b}_{?}$, logo, a afirmação é Verdadeira. ?

FALTOU ACHAR K com $a - b = 7 \cdot n \cdot K$?

X

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

evite "sendo". Aqui: "para algum"

Se $a \equiv b \pmod{42}$, logo: $a - b = 42K$, sendo $K \in \mathbb{Z}$. No entanto, temos que: $126 \equiv 84 \pmod{42}$ e $126 > 42$, assim como $84 > 42$. Logo, a afirmação é falsa. Muito bem!

($a := 84$, $b := 84$ serve também).

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

evite essas setinhas

Dos dados fornecidos podemos concluir que:

(i) $a \equiv b \pmod{n} \to n \mid a - b \to \boxed{a - b = nK_1}$, sendo $K_1 \in \mathbb{Z}$

(ii) $b \equiv c \pmod{n} \to n \mid b - c \to \boxed{b - c = nK_2}$, sendo $K_2 \in \mathbb{Z}$

Somando (i) e (ii), temos:

$$a - c = nK_1 + nK_2$$

$$c - a = -n(K_1 + K_2)$$

Portanto, podemos concluir que $c \equiv a \pmod{n}$ é Verdadeiro, já que a soma dos inteiros K_1 e K_2, também ~~...~~ resulta em um inteiro

Cuidado: teu inteiro aqui seria o $-(k_1+k_2)$, e não o k_1+k_2.

✓

Correto!

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
Prova ou Refutação.

REFUTAÇÃO:

Prova por exaustão?

TOME $a=0$, $b=2$, $n=2$ ✓

LOGO $a \equiv b \pmod{n}$, POIS $2 \mid 2-0$, POIS $2.1=2$ ✓

"Mas" — ~~LOGO~~ $a \not\equiv b \pmod{7n}$, POIS $14 \nmid 2-0$, POIS $\nexists k \in \mathbb{Z}$ t.q. $14k=2$ ✓

LOGO PARA TODO $a, b, n \in \mathbb{Z}$ COM $n>1$, $a \equiv b \pmod{n} \not\Rightarrow a \equiv b \pmod{7n}$

↳ ERRADO! Ache uma nova refutação disso!

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \le 42$ ou $b \le 42$.
Prova ou Refutação.

REFUTAÇÃO:

TOME ~~[illegible]~~, ~~[illegible]~~ $a=85$, $b=43$

NOTE QUE $a \equiv b \pmod{42}$, POIS $42 \mid 42$ $[85-43=42]$

PORÉM $85 \not\le 42$ E $43 \not\le 42$ ✓

Prova por exaustão?

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
Prova ou Refutação.

PROVA:

NOTE QUE $\exists k' \in \mathbb{Z}$ t.q. $n.k' = a-b$ [i]

NOTE QUE $\exists k'' \in \mathbb{Z}$ t.q. $n.k'' = b-c$ [ii]

Pela (i), ~~NOTE QUE~~ $b = n.k'' + c$ PARA ALGUM $k'' \in \mathbb{Z}$

pela (ii), ~~NOTE QUE~~ $nk' = a - (n.k'' + c)$ PARA ALGUNS $k', k'' \in \mathbb{Z}$

já "seja" teu k'!

MANIPULANDO... $nk' = a - nk'' - c$

SSE $nk' + nk'' = a - c$

SSE $n(k'+k'') = a-c$

a prova teria que ser: $n \mid c-a$. Você provou que $n \mid a-c$. } exatamente!

NOTE QUE $(k'+k'') \in \mathbb{Z}$ PELA PROPRIEDADE DE + EM $\mathbb{Z}$

↳ ???

LOGO $\exists k \in \mathbb{Z}$ t.q. $nk = a-c$

LOGO $n \mid a-c$

LOGO $a \equiv c \pmod{n}$ ✓

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

REFUTAÇÃO:

Seja $a, b, n \in \mathbb{Z}$:

$n = 2$

$a = 5$

$b = 1$

$a \equiv b \pmod{n}$

$2 \mid 5 - 1$ ✓

$a \equiv b \pmod{7n}$

$7 \cdot 2 \mid 5 - 1$

$14 \mid 5 - 1$ X

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

PROVA:

Seja $a, b \in \mathbb{Z}$:

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

essas duas proposições não têm papeis iguais aqui.
Olha:

D

Prove ou refuta as afirmações:

o que significam?

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

"...para algum..."

$7n \mid a-b \Leftrightarrow (a-b) = 7n \cdot q_1$ I
$n \mid a-b \Leftrightarrow (a-b) = n \cdot q_2$ II, igualando
$7n \cdot q_1 = n \cdot q_2$, e só será verdade quando $q_2 = 7q_1$
logo a hipotese é falsa.

use isso para mostrar um contraexemplo.

OK

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

evite!

i $\Leftrightarrow n \mid (a-b) \Leftrightarrow a-b = q_1 \cdot n$ } de ii temos $b = q_2 n + c$
ii $\Leftrightarrow n \mid (b-c) \Leftrightarrow b-c = q_2 \cdot n$ } substituindo em i:
$\Leftrightarrow a - (q_2 n + c) = q_1 n \Leftrightarrow a - q_2 \cdot n - c = q_1 n$
$\Leftrightarrow a - c = q_1 n + q_2 n$ } $\Leftrightarrow c - a = -(n \cdot (q_1 + q_2))$
$c - a = -n \cdot q_3$ ← onde ($q_3 = q_1 + q_2$)
isso significa que a hipotese é falsa, pois o quociente não pode ser negativo.

(1) por que não?
(2) sobre nenhum dos sabemos se é negativo ou não.

ERRADO, A HIPÓTESE É VERDADEIRA. → mas o que foi o erro?

$q_1 \cdot n = a - b$
$q_2 \cdot n = b - c$ } SOMANDO → $2n \cdot q_1 \cdot q_2 = a - c$
$n(2 \cdot q_1 \cdot q_2) = a - c$
$n \mid a - c \Rightarrow c \equiv a \pmod{n}$

Na verdade, o que tu escreveu realmente é uma prova do "D3"! (Que realmente é válido, e tua prova 100% correta!)

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

$a \equiv b \pmod{n} \Rightarrow n \mid a-b$
$a \equiv b \pmod{7n} \Rightarrow 7n \mid a-b$
Suponha $a = 6$, $b = 2$ e $n = 2$, temos que $2 \mid 6-2$,
mas $7 \cdot 2 \nmid 6-2$. (contra-exemplo)

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

?

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

"para algum"

Temos que
(I) $a \equiv b \pmod{n} \Rightarrow n \mid a-b \Rightarrow n \cdot q = a-b$, com $q \in \mathbb{Z}$
(II) $b \equiv c \pmod{n} \Rightarrow n \mid b-c \Rightarrow n \cdot p = b-c$, com $p \in \mathbb{Z}$

Logo,
$nq + np = a - b + b - c$
$= n(q+p) = a - c \Rightarrow n \mid a-c$ $(p+q \in \mathbb{Z})$
$\Rightarrow a \equiv c \pmod{n}$

Portanto, $c \not\equiv a \pmod{n}$

Cuidado!

Tente provar que: $x \equiv y \pmod{n} \Leftrightarrow y \equiv x \pmod{n}$.

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

$2 \equiv 4 \pmod{2}$, mas $2 \not\equiv 4 \pmod{7*2}$

Falso.

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

$84 \equiv 420 \pmod{42}$, mas $84 > 42$ e $420 > 42$

Falso.

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

??

(iii) $m \mid (a-b) \Leftrightarrow mq' = (a-b)$

(iv) $m \mid (b-c) \Leftrightarrow mq'' = (b-c)$

$q \neq$ parece rascunho

$m \mid (c-a)$?

$\hookrightarrow$ sse $(\exists\, q'''_{\in ?}\ t_q\ mq''' = (c-a))$

$b = -mq' + a$

$\to q'''$

$mq'' = mq' + a - c$

$mq'' + mq' = a - c \Rightarrow -m(q' + q'') = (c-a) = m(-q' - q'') = c - a$

~~[illegible]~~ $\boxed{m \cdot q''' = c - a}$

Cuidado!

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

Refutação: $a = 5$, $b = 2$, $n = 4$ $5 \not\equiv 2 \pmod 4$!
"Onde"? Temos $a \equiv b \pmod{7n}$,
Onde $5 \equiv 2 \pmod{28}$, Cuidado.
Portanto, $28 \nmid 3$ ~~ou~~ $\cancel{n(28 \mid 3)}$.

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

$a = 84$, $b = 42$ NÃO PROVA PARA TODO VALOR
Temos $a \equiv b \pmod{42}$
Onde $84 \equiv 42 \pmod{42}$
Logo, $42 \mid 42$. ?? o que isso tem a ver?

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

$a = 16$, $b = 8$, $c = 4$; $n = 2$
Temos X

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

$nk = a - b$

Sejam a, b e n ∈ ℤ com n>1. Suponha que a ≡ b (mod n), ou seja, n | a−b, portanto, $\boxed{(a-b)k = n}$ ~~para~~ algum k inteiro pelas definições 1 e 2 respectivamente. Disso temos que (a−b)k·7 = 7·n. Como os inteiros são fechados pela multiplicação, k·7 é inteiro. Logo, existe um inteiro q, onde q = 7k, tal que (a−b)q = 7n, ou seja, 7n | a−b, ou seja a ≡ b (mod 7n).

a−b | 7n

Ok

Cuidado!

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \le 42$ ou $b \le 42$.
PROVA OU REFUTAÇÃO.

Esta afirmação está errada. Suponha que a = 44 e b = 86. Dessa forma, temos que a ≡ b (mod 42), pois 42 | 44 − 86 ~~[illegible]~~ ("... mas nem 44 ≤ 42 nem 86 ≤ 42")

Obs: poderia tomar a := 44, b := 86 também!

Ok

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

Suponha que a ≡ b (mod n) e que b ≡ c (mod n), ou seja, n | a−b e n | b−c, pela definição 2. Disso temos que (a−b)k = n, para algum k inteiro, e que (b−c)k' = n, para algum inteiro k', pela ~~de~~ definição 1.

...?

Não terminado!

$a \equiv b \pmod{m}$ | $m \mid a - b$

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
Prova ou Refutação.

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
Prova ou Refutação.

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
Prova ou Refutação.

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

A afirmação é falsa. Contraexemplo:
Para $a=2$, $b=0$ e $n=2$, temos que $2 \equiv 0 \ (\text{mod } 2)$
$2 \mid 2-0$, definição de $\equiv$
$2 \mid 2$, $2.1=2$

Mas não temos $2 \equiv 0 \ [\text{mod}(7.2)]$, pois $2 \equiv 0 \ (\text{mod } 14)$
$14 \mid 2-0$, definição de $\equiv$
$14 \nmid 2$, não existe $q \in \mathbb{Z}$ tal que $14.q=2$

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

A afirmação é falsa. Contraexemplo:
Para $a=43$ e $b=43$, temos que: $43 \equiv 43 \ (\text{mod } 42)$
$42 \mid 43-43$, pela definição de $\equiv$
$42 \mid 0$, ~~verdade~~ pela prova em C2

Mas não temos $a \leq 42$ ou $b \leq 42$.

perfeito!

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

alguns

Se (i) e (ii), então $n \mid a-b$ e $n \mid b-c$, definição de $\equiv$
$n.q_1 = a-b$ e $n.q_2 = b-c$, definição de $\mid$, para $q_1, q_2 \in \mathbb{Z}$
? $n.q_1 = a - n.q_2 - c$
? $n q_1 + n q_2 = a-c$
? $n(-q_1-q_2) = \cancel{a-c}$ $c-a$
...

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

Refutação:
(?) $8 \equiv 4 \bmod (2)$
(?) $2 \mid 8-4 \Rightarrow 2 \mid 4$ (Verdade)
Porém
~~8~~ $8 \not\equiv 4 \bmod (7 \cdot 2)$
(?) $14 \mid 4$ (falso)

idéia correta.
parece rascunho.

Como o exemplo ao lado podemos ver que a afirmação é falso.

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

Refutação:
~~[illegible]~~
(?) $126 \equiv 84 \pmod{42}$
(?) $42 \mid 126-84$
(?) $42 \mid 42$ (Verdadeiro)

idéia correta!
cuidado na escrita

Logo, podemos concluir que não necessariamente a ou b precisam ser maiores ou iguais a 42.

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

?

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

Refutação porem

$a = 1$

$b = 3$

$n = 2$

$1 \equiv 3 \ (\text{mod } 2)$ ✓ $\quad 1 \not\equiv 3 \ (\text{mod } 14)$

C

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

Refutação

$a = 43$

$b = 85$

$43 \equiv 85 \ (\text{mod } 42) \wedge 42 < 43 \quad 42 < 85$

✓ Perfeito! (Poderia tomar $a := 43$, $b := 43$ também.)

C

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

Prova $f \in \mathbb{Z}$

$n \mid a - b$

$n \mid b - c$ $\quad$ logo $n \mid c - a$?

$(a-b) \cdot f_1 = n \quad a f_1 - b f_1 = b f_2 - c f_2$

$(b-c) \cdot f_2 = n \quad b f_1 + b f_2 = a f_1 + c f_2$

$(a-c)\, f_3 = n$

o que são essas equações e esses b_1, b_2, b_3?

C

D

Prove ou refuta as afirmações:

trabalhou com todos os detalhes que aqui não seria necessário. (veja o gabarito)

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

Refutação: Para $a = 8$, $b = 6$ e $n = 2$, temos que $8 \equiv 6 \pmod 2$ é verdade pois $a \equiv b \pmod n \iff n \mid a - b$, ou seja, $n \cdot q = a - b$, com $q \in \mathbb{Z}$ e tal q existe e é $1 \Rightarrow 2 \cdot 1 = 8 - 6$. Porém para $a \equiv b \pmod{7n}$ temos $8 \equiv 6 \pmod{14}$ que é falso, pois não existe q tal que $14 \cdot q = 8 - 6$. correto!

pode existir mais de um q

realmente a frase "e é 1" fica estranha. Um "por exemplo" seria melhor, ou simplesmente escreva: "Observe que $2 \cdot 1 = 8-6$..."

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO. "existe"

~~Refutação~~
Prova: Para $a = 43$ e $b = 1$ (ou $b = 43$ e $a = 1$) temos que $43 \equiv 1 \pmod{42}$ é verdade pois $\exists q$ tal que $42 \cdot q = 43 - 1$, com $q \in \mathbb{Z}$, porém $a > 42$, logo temos um absurdo pois é impossível que $\overset{a-b}{a \leq 42}$ e ao mesmo tempo $a > 42$, portanto a premissa é verdadeira.

é uma refutação ✓

o que é esse q? sim. $(\exists q \in \mathbb{Z})$...

Neste caso $b \leq 42$ e satisfaz o enunciado.

exatamente! cuidado!

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

Prova:
Se $a \equiv b \pmod n$, então temos que $n \cdot q = a - b$, com $q \in \mathbb{Z}$.
Se $b \equiv c \pmod n$, " " " $n \cdot q = b - c$, " " ".
Se $c \equiv a \pmod n$, " " " $n \cdot q = c - a$, " " ".
Como sabemos que $n \cdot q = a - b$ e $n \cdot q = b - c$, temos que:

$$a - b = b - c = c - a, \text{ logo } a - b = c - a.$$

Não necessariamente esse q sempre vai ser o mesmo, não podemos supor que são.

cuidado pois...

D

O correto seria: "No entanto $k \notin \mathbb{Z}$"

Prove ou refuta as afirmações:

O que é esse k?

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

Falso. Tome $a = 5$, $b = 9$ e $n = 4$. Daí, $4k = 5 - 9 \Rightarrow k = -1$. Porém, $7 \cdot 4k = -4$
$k = \frac{-4}{28}$. No entanto, $k \in \mathbb{Z}$.

incorreto! (pense porque!)

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

Falso. Tome $a = 100$ e $b = 58$. Daí,
$42 \mid (100 - 58) \Leftrightarrow 42k = 42 \Leftrightarrow k = 1$.

e daí?

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

$a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b) \Leftrightarrow n k_1 = a - b$
e $b \equiv c \pmod{n} \Leftrightarrow n \mid (b - c) \Leftrightarrow n k_2 = b - c$.
Daí, $a = b + n k_1$ e $b = c + n \cdot k_2$.
Logo, $a = c + n \cdot k_2 + n \cdot k_1 \Leftrightarrow a - c = n(k_1 + k_2)$

Obs: queremos $c - a = \cdots$ e não $a - c = \cdots$.

OBS: onde k_1 e $k_2 \in \mathbb{Z}$.

estranho

D

Prove ou refuta as afirmações:

D1 Para todo $a, b, n \in \mathbb{Z}$ com $n > 1$, se $a \equiv b \pmod{n}$ então $a \equiv b \pmod{7n}$.
PROVA OU REFUTAÇÃO.

CONSIDERANDO QUE $n \mid a-b \Rightarrow a-b = n \cdot q$, ONDE $q \in \mathbb{Z}$, ENTÃO:
SEJA $K \in \mathbb{Z}$ e $K = 7 \cdot q$, TEMOS QUE $7n \mid a-b \Rightarrow a-b = 7 \cdot n \cdot q \Rightarrow$
$\Rightarrow a-b = n \cdot 7 \cdot q \Rightarrow a-b = n \cdot K$

aqui $k=q$ e não $k=7q$.

?

PORTANTO $a \equiv b \pmod{7n}$

?

D2 Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{42}$ então $a \leq 42$ ou $b \leq 42$.
PROVA OU REFUTAÇÃO.

E

D3 Sejam a, b, c, n inteiros com $n > 1$, tais que:

(i) $a \equiv b \pmod{n}$;

(ii) $b \equiv c \pmod{n}$.

Logo $c \equiv a \pmod{n}$.
PROVA OU REFUTAÇÃO.

para algum

PARTINDO de $n \mid a-b$ e $n \mid b-c$, TEMOS:
$a-b = n \cdot q$, ONDE $q \in \mathbb{Z}$
$\boxed{b = (n \cdot q) + a}$??? cuidado!
SUBSTITUIREMOS b em $b-c = n \cdot x$, onde $x \in \mathbb{Z}$, temos
$(n \cdot q) + a - c = n \cdot x$?
$a - c = (n \cdot x) - (n \cdot q)$?
$c - a = (n \cdot q) - (n \cdot x)$
$c - a = n(q - x)$, $x \in \mathbb{Z}$
$c - a = n \cdot x$ ✓

não precisa dar nome.

Portanto $c \equiv a \pmod{n}$

C