(24) **I**

Sejam m_1, m_2 inteiros coprimos.

(12) **I1.** O sistema de congruências seguinte possui resolução:

$$x \equiv b_1 \pmod{m_1} \qquad x \equiv b_2 \pmod{m_2}$$

(12) **I2.** Ainda mais, tal resolução é única módulo $m_1 m_2$.

(3) Enunciado de **I1**. (Podes escrever em português matemático ou usando fórmula mesmo.)

0

$\text{rem}(x, m_1) = \text{rem}(x, m_2)$

(9) Demonstração de **I1**.

Sejam m_1, m_2 inteiros tais que $(m_1, m_2) = 1$, b_1, b_2 inteiros e x t.q.

$x \equiv b_1 \pmod{m_1}$ e $x \equiv b_2 \pmod{m_2}$

$x \equiv b_1 \pmod{m_1}$ e $x \equiv b_2 \pmod{m_1}$

$\Rightarrow \exists k \mid m_1 k = x - b_1$ $\Rightarrow \exists k' \mid m_2 k' = x - b_2$

$\begin{cases} m_1 k = x - b_1 \\ m_2 k' = x - b_2 \end{cases} \Rightarrow m_1 m_2 (k k') = (x - b_1)(x - b_2)$

$(x - b_1)(x - b_2) \equiv 0 \pmod{m_1 m_2}$

confundiu implicação com inferência?

misturou notação de conjuntos com fórmulas? (nunca use isso!)

(4) Enunciado de **I2**. (Podes escrever em português matemático ou usando fórmula mesmo.)

4

$\forall x_1, x_2, m_1, m_2 \left((x_1 \equiv_{m_1} b_1 \;\&\; x_1 \equiv_{m_2} b_2) \;\&\; (x_2 \equiv_{m_1} b_1 \;\&\; x_2 \equiv_{m_2} b_2) \right) \Rightarrow x_1 \equiv x_2 \pmod{m_1 m_2}$

(8) Demonstração de **I2**.

1

Suponha x_1, x_2 t.q. $x_1 \equiv_{m_1} b_1$, $x_1 \equiv_{m_2} b_2$, $x_2 \equiv_{m_1} b_1$ e $x_2 \equiv_{m_2} b_2$

$x_1 \equiv_{m_1} b_1$

Só isso mesmo.

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

(6) Sejam x, y, m inteiros, dizemos que x e y são congruentes módulo m se e somente se $m \mid x-y$.

Precisa ponto final aqui!

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[x \equiv y \pmod m]\,.$$

(6) DEMONSTRAÇÃO.

(2) Sejam x, y inteiros.
Suponha que $x \equiv y \pmod 0$. (1)
Seja m inteiro tal que $m \geq 0$.
Quero mostrar que $x \equiv y \pmod m$.

Caso $m = 0$:
Imediata por (1).
Caso $m > 0$:
Quero mostrar que $(\exists k)[m = (x-y)\cdot k]$

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$. Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: *Não tenha medo aplicar as definições das relações envolvidas.*

DEMONSTRAÇÃO:

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

5

para todo, x, y, m: int. x é congruente y módulo m $\Leftrightarrow$ se m divide $x - y$.

isso tem cara de Prop, não de definição!

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[x \equiv y \pmod m]\,.$$

(6) DEMONSTRAÇÃO.

(3)

Suponha ~~$x = 0$~~ $x \equiv y \pmod 0$;
Logo, $0 \mid x - y$, logo $x = y$;
Como $x = y$, logo ~~$x \underset{m}{\equiv} y$ para qualquer $m > 0$~~ $x \underset{m}{\equiv} y$ para qualquer $m \geq 0$.

↳ por quê??

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$.
Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: *Não tenha medo aplicar as definições das relações envolvidas.*

DEMONSTRAÇÃO:

(12) **G**

Esse contexto não faz sentido para definir uma relação ternária!

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

1

Sejam $a, b, m, q_a, q_b, r_a, r_b \in \mathbb{Z}$
t.q $a = mq_a + r_a$ e $b = mq_b + r_b$. ← isso não é suficiente para ter que teus q's e r's são quocientes e restos.
$a \equiv b \pmod m \overset{\text{def}}{\iff} r_a = r_b$.

também.

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[x \equiv y \pmod m]\,.$$

(6) DEMONSTRAÇÃO.

indemonstrável.

0

Suponha $X \equiv Y \pmod 0$.
Seja $m \geqslant 0$.
Como $X \equiv Y \pmod 0$, logo $X = 0 \cdot q_x + r_x$ e $Y = 0 \cdot q_y + r_y$, logo $X = r_x$ e $Y = r_y$.
Como $X \equiv Y \pmod 0$, logo $r_x = r_y$, logo $X = Y$.
Como $X = Y$, logo $mq_x + r_x = mq_y + r_y$, logo $r_x = r_y$, logo $X \equiv Y \pmod m$.

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$.
Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: *Não tenha medo aplicar as definições das relações envolvidas.*

DEMONSTRAÇÃO:

Dentro do texto da tua definição sequer apareceu o termo que é pra ser definido.

Está afirmando ou definindo?

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

Sejam a e b inteiros. Existe um u tal que u multiplicado com m somado a a é igual a b.

quem é m?

contexto errado.

isso é mais legível/claro que « um+a = b» ?!

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[x \equiv y \pmod m]\,.$$

(6) DEMONSTRAÇÃO.

Sejam x, y : Int.
Suponha $x \equiv y \pmod 0$.
Então existe u. $u \cdot 0 + x = y$.
Suponha $0 \neq 0$.
Portanto $u \cdot 0 + x = y$.

Ou seja, $x = y$.
Segue que basta encontrar u que multiplicado a um m qualquer, tenha $u \cdot m + x = y$.
Portanto, suponha $0 = 0$.
$0 \cdot m + x = y$
$\Rightarrow x = y$.

quem é?

Não quero supor isso.

o que significa « u multiplicado a um m qualquer» ?!?

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$. Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: Não tenha medo aplicar as definições das relações envolvidas.

DEMONSTRAÇÃO:

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

(6) Sejam a, b e m inteiros, tal que $m \geq 0$. O a é congruente ao b no módulo m se, e somente se, m divide o a menos o b.

ouch!

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[x \equiv y \pmod m]\,.$$

quem é k?

(6) DEMONSTRAÇÃO.

4 Seja x e y inteiros, t.q. $x \equiv y \pmod 0$, ou seja $0k = x - y$.
Seja m inteiro, t.q. $m \geq 0$.
Calculemos:
$x - y = 0k$
$= 0$
$= m0$. ..e?

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$.
Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: Não tenha medo aplicar as definições das relações envolvidas.

DEMONSTRAÇÃO:

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

CADÊ O CONTEXTO?

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

(6) Dizemos que dois inteiros a, b são congruentes módulo um inteiro m, se e somente se $m \mid a-b$. Em símbolos:

$$a \equiv_m b \iff m \mid a-b.$$

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[x \equiv y \pmod m]\,.$$

(6) DEMONSTRAÇÃO.

(4) Seja y inteiro t.q $x \equiv y \pmod 0$. ✓
Temos $0 \mid x-y$ logo $x-y=0$. ✓
Logo $x=y$.
Seja m inteiro t.q $m \geq 0$. ✓
Imediato. ✗ → Não é!

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$. Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: Não tenha medo aplicar as definições das relações envolvidas.

DEMONSTRAÇÃO:

Seja m inteiro t.q $(m, n) = 1$
Temos $(m^e)^d = m^{ed}$
Temos $m^{ed} = m \cdot m^{(ed-1)}$
Basta $m^{ed-1} \equiv 1 \pmod n$.
∴
⋮
Como $m^{ed-1} \equiv 1 \pmod n$ logo $(m^e)^d \equiv m \pmod n$.

(12) **G** Escolho G p/ correção

Type error: Prop!!

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

(6)

$(\forall x, y, n \text{ int})\ \{ x \equiv y \pmod n \text{ sse } n \mid x-y \}$

Sejam x, y, n int. x é congruente a y módulo n se, e somente se, n divide $x-y$.

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[x \equiv y \pmod m]\,.$$

quem é

quem é?

(6) DEMONSTRAÇÃO.

Qual teu alvo neste momento?

(3)

Seja m int t.q. $m \geq 0$

Se $x \equiv y \pmod 0$, pela definição de congruência temos que $0 \mid x-y$, o que só acontece se $x-y = 0$. Para $x \equiv y \pmod m$ temos que $m \mid x-y$, substituindo chegamos que $m \mid 0$ ... e?

(36) **H**

Não é para escrever Props aqui!! Cadê o código?! ☹

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$. Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: Não tenha medo aplicar as definições das relações envolvidas.

DEMONSTRAÇÃO:

Seja d int t.q. $ed \equiv 1 \pmod{\varphi(n)}$. ☹

Por definição de congruência temos que $\varphi(n) \mid ed - 1$

Seja m int t.q. $(\forall m, n) = 1\ \{(m^e)^d \equiv m \pmod n\}$

Como $(m, n) = 1$, Pela lei do cancelamento

$(m^e)^{d-1} \equiv 1 \pmod n$

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

6

Sejam a, b, m inteiros e $m \geq 0$,

$a \equiv b \pmod m \overset{\text{def}}{\iff} m \mid b-a$

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[\,x \equiv y \pmod m\,]\,.$$

(6) DEMONSTRAÇÃO.

5

Suponha $x \equiv y \pmod 0$
Seja k: int t.q. $0k = y - x$
Logo $0 = y - x$ [? Am]
Logo $x = y$ (1) [ZA. Para]

Seja m: int t.q. $m \geq 0$
Calcule:
$x \equiv x \pmod m$ [reflexividade]
$\equiv y \pmod m$ [pelo (1)]

cadê?

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$. Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: *Não tenha medo aplicar as definições das relações envolvidas.*

DEMONSTRAÇÃO:

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

(6)

Sejam x, y, m inteiros. Se $m \mid x-y$ então x é congruente a y módulo m.

isso tem cara de Prop

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[x \equiv y \pmod m]\,.$$

(6) DEMONSTRAÇÃO.

(6)

Seja y inteiro tal que $x \equiv y \pmod 0$. ✓
Seja m tal que $m \geq 0$. ✓
Como $x \equiv y \pmod 0$, logo $0 \mid x-y$, portanto pela forma legal $x-y=0$. ✓
Logo, $x \equiv y \pmod m$, já que $m \mid 0$. ✓

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$.
Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: *Não tenha medo aplicar as definições das relações envolvidas.*

DEMONSTRAÇÃO:

(12) **G**

Prop!

→ contexto errado para definir relação ternária

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

2

SEJA a INTEIRO. PARA QUALQUER m INTEIRO, SE EXISTE $b = q$ INTEIROS TAL QUE $b = a - m \cdot q$, DIZEMOS QUE a É CONGRUENTE A b EM MODULO DE m.

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[\,x \equiv y \pmod m\,].$$

(6) DEMONSTRAÇÃO.

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$. Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: Não tenha medo aplicar as definições das relações envolvidas.

DEMONSTRAÇÃO:

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

(6) Seja m um inteiro.
Temos que para quaisquer a e b inteiros a vai ser congruente módulo m sse ~~$m \mid b$~~ $m \mid a-b$. Em símbolos:
$(\forall a,b)[a \equiv b \pmod m \overset{\text{def}}{\Leftrightarrow} m \mid a-b]$

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[x \equiv y \pmod m]\,.$$

(6) DEMONSTRAÇÃO.

(6) Suponha $x \equiv y \pmod 0$.
Seja k t.q. $0.k = x-y$.
Como $0 = x-y$, logo, $x = y$.
~~Calculamos:~~
Seja $m \geq 0$.

Calculamos:
$x \equiv x$ (Reflexividade congruência).
Logo $x \equiv y$ ($x = y$) ✓

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$.
Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: *Não tenha medo aplicar as definições das relações envolvidas.*

DEMONSTRAÇÃO:

(12) **G**

escolha bizarra!

Infelizmente eu escolhi a G

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

6

Sejam a, b, m inteiros. Dizemos que a é congruente a b módulo m e escrevemos $a \equiv_m b$ se, e somente se, $m \mid a-b$.

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[x \equiv y \pmod m]\,.$$

(6) DEMONSTRAÇÃO.

6

Seja y inteiro tal que $x \equiv_0 y$. Logo, seja k tal que $0 \cdot k = x - y$. Logo, temos $0 = x - y$ [zero anulador]. ~~Logo, $x = y$ [Unicidade dos inversos aditivos.],~~ Seja m inteiro e maior ou igual a zero. ~~Como $x - y = 0$, logo, $m \mid x - y$~~ Use 0 como testemunha. Ele gera anuladores, $m \cdot 0 = 0$. Logo, 0 $m \mid x - y$.

(36) **H** → Seja $m \geq 0$. !!

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$. Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: Não tenha medo aplicar as definições das relações envolvidas.

DEMONSTRAÇÃO:

Seja m tal que $(m, n) = 1$.

Como logo Calculemos

$(m^e)^d = m^{e \cdot d}$

$\equiv m^{ed}$ (mod ?)

$\equiv m^1$ (mod $\varphi(n)$) [definição de inverso mod m]

Definição de inverso mod $\varphi(n)$

$\equiv_{\varphi(n)} m$

∴

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

(5)

Sejam a, b, m inteiros com $m > 0$. Dizemos que a e b são congruentes módulo m, se e somente se, $m \mid a-b$.

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[x \equiv y \pmod m]\,.$$

(6) DEMONSTRAÇÃO.

(2)

Seja y inteiro.
Suponha $x \equiv y \pmod 0$.
Seja m inteiro tal que $m \geq 0$.
$x \equiv y \pmod 0 \Rightarrow 0 \mid x-y$

$0 \mid x-y \Rightarrow (\exists k)[0k = x-y]$
$x - y = 0$ (ZM-IdL)
$x = y$.
$x = y \Rightarrow x \equiv y \pmod m$

(36) **H** Type error. O que uma Prop tá fazendo solta aqui?

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$. Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: *Não tenha medo aplicar as definições das relações envolvidas.*

DEMONSTRAÇÃO:

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

(6) Sejam a, b, m inteiros tal que $m > 0$, dizemos que a e b são congruentes módulo m se e somente se $m \mid a-b$. Em símbolos:

$$a \equiv b \pmod{m} \overset{\text{def}}{\iff} m \mid a-b$$

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod{0} \implies (\forall m \geq 0)\,[\,x \equiv y \pmod{m}\,].$$

(6) DEMONSTRAÇÃO.

1 Sejam x, y inteiros tais que $x \equiv y \pmod 0$ (1)
Logo $0 \mid x-y$. Contradição.

↳ o que significa $0 \mid x-y$ mesmo??

$0 \mid x-y \iff$??

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$. Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod{n}.$$

Dica: Não tenha medo aplicar as definições das relações envolvidas.

DEMONSTRAÇÃO:

(24) **I**

Sejam m_1, m_2 inteiros coprimos.

(12) **I1.** O sistema de congruências seguinte possui resolução:

$$x \equiv b_1 \pmod{m_1} \qquad x \equiv b_2 \pmod{m_2}$$

(12) **I2.** Ainda mais, tal resolução é única módulo $m_1 m_2$.

(3) ENUNCIADO DE **I1**. (Podes escrever em português matemático ou usando fórmula mesmo.)

× equivalente ao b_2 caso o modulo de m1 ?

(9) DEMONSTRAÇÃO DE **I1**.

$a^{\phi(n)} \equiv (\mathrm{mod}\ n)$ a congruência utiliza o Teorema de Euler para

apresentar esse sistema ?

nada disso faz sentido.. :-:

(4) ENUNCIADO DE **I2**. (Podes escrever em português matemático ou usando fórmula mesmo.)

× equivalente ao b_2 caso o modulo de m_2

(8) DEMONSTRAÇÃO DE **I2**.

$a^{\phi(m)} \equiv (\mathrm{mod}\ m)$ essa congruência também utiliza o Teorema de

Euler da mesma forma como a da demonstração anterior

?!

Só isso mesmo.

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[\,x \equiv y \pmod m\,].$$

(6) DEMONSTRAÇÃO.

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$.
Demonstre que para todo m com $(m, n) = 1$,

30

$$(m^e)^d \equiv m \pmod n.$$

Dica: *Não tenha medo aplicar as definições das relações envolvidas.*

DEMONSTRAÇÃO:

Seja $m : Int$ t.q $(m,n)=1$ ✓

Seja $k : Int$ t.q $\varphi(n)\cdot k = ed-1$ ✓

Calculamos:

$(m^e)^d = m^{ed}$

$= m^{ed-1} \cdot m$

$= m^{\varphi(n)k} \cdot m$ [Pela escolha de k]

$= (m^{\varphi(n)})^k \cdot m$

Temos que $m^{\varphi(n)} \equiv 1 \pmod n$. ✓
[Teorema de Euler]

Logo, $(m^{\varphi(n)})^k \equiv_n 1^k$. ✓

Como $1^k \equiv_n 1$, então ✓

$(m^{\varphi(n)})^k \equiv_n 1$. ✓

Logo $(m^{\varphi(n)})^k \cdot m \equiv_n m$. ✓

Logo $(m^e)^d \equiv_n m$. ✓

∎

Teorema de Euler:

$(\forall n, m)\left[(n,m)=1 \Rightarrow m^{\varphi(n)} \equiv_n 1\right]$

Sejam n, m : Int tal que $(n,m)=1$.

Seja R_n : Set (Int) um S.R.R mod n.

Logo mR_n é um S.R.R mod n. (?)

Logo $mR_n \equiv_n R_n$. ✓

Logo, $\prod_{x \in mR_n} x \equiv_n \prod_{y \in R_n} y$.

Logo, $m^{\varphi(n)} \cdot \prod_{x \in R_n} x \equiv_n \prod_{y \in R_n} y$.

Logo, $m^{\varphi(n)} \equiv_n 1$. (Pois $(\forall x \in R_n)[(x,n)=1]$) (?)

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

5

Sejam a, b inteiros
Seja $m > 0$
Então $a \equiv b \pmod{m} \iff m \mid a - b$

Parece demonstração.

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod{0} \implies (\forall m \geq 0)\,[x \equiv y \pmod{m}]\,.$$

(6) DEMONSTRAÇÃO.

1

Sejam x, y inteiros
Suponha $x \equiv y \pmod{0}$
Seja $m, n \in \mathbb{Z}$ inteiros $x - y = 0 \cdot n + 0$
Então $x = y$, portanto $[x \equiv y \pmod{v}](\forall v \geq 0)$

Qual é teu alvo neste momento?

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$. Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod{n}.$$

Dica: Não tenha medo aplicar as definições das relações envolvidas.

DEMONSTRAÇÃO:

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

6

Sejam a, b, m inteiros. Dizemos que a é congruente a b módulo m sse $m \mid a-b$.

Teorema. Seja 6 inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[x \equiv y \pmod m]\,.$$

$m \cdot \square = x - y$.

(6) DEMONSTRAÇÃO.

(6)

Sejam 6 x, y : int t.q $x \equiv y \pmod 0$.
Seja m : int t.q $m \geq 0$.
Como $x \equiv y \pmod 0$, logo $0 \mid x-y$. [def. congruência]
Logo $x = y$. [Z-MZ0]
Logo $x - y = 0$. [ZA-INVR]
Logo $m \cdot 0 = 0$. [Z-ZERO/mul]
Uso 0 como testemunha.

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$. Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Esse "Logo" não faz sentido.

Dica: *Não tenha medo aplicar as definições das relações envolvidas.*

DEMONSTRAÇÃO:

(12) **G**

Parece Prop

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

(6)

Sejam

Para todo $a, b, m \in \mathbb{Z}$. Dizemos que a é congruente b módulo m se $m \mid a - b$. Em símbolos, temos:

$(\forall a, b, m \in \mathbb{Z})[\, a \equiv b \pmod{m} \overset{\text{def}}{\iff} m \mid a - b \,]$.

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod{0} \implies (\forall m \geq 0)\,[x \equiv y \pmod{m}]\,.$$

(6) DEMONSTRAÇÃO.

6

Seja y inteiro t.q. $x \equiv y \pmod 0$.
Seja m inteiro t.q. $m \geq 0$.
Como $m \mid 0$ e $0 \mid x - y$, logo $m \mid x - y$. [Propriedade transitiva de $\mid$]
Portanto, $x \equiv y \pmod m$.

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$. Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod{n}.$$

Dica: Não tenha medo aplicar as definições das relações envolvidas.

DEMONSTRAÇÃO:

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

6 Sejam a, b, m inteiros. Diremos que a é congruente (~~mod~~) a b módulo m se (~~m~~) $m \mid a-b$.

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[\,x \equiv y \pmod m\,].$$

(6) DEMONSTRAÇÃO.

4 Sejam x, y inteiros. Suponha que $x \equiv y \pmod 0$. (1) Disso, pela definição de módulo segue que $x - y = 0$. Já que $0 \neq$ inteiro $\neq 0$. Suponha m inteiro tal que $m \geq 0$. Vou mostrar que $x \equiv y \pmod m$. (~~Colocando~~) Por (1) temos que $x - y = 0$, assim para todo inteiro m segue que $m \mid 0$ (pois 0 é divisível por qualquer número).

(36) **H** → RASCUNHÍSSIMO

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$. Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: *Não tenha medo aplicar as definições das relações envolvidas.*

DEMONSTRAÇÃO:

(24) **I**

Sejam m_1, m_2 inteiros coprimos.

(12) **I1.** O sistema de congruências seguinte possui resolução:

$$x \equiv b_1 \pmod{m_1} \qquad x \equiv b_2 \pmod{m_2}$$

(12) **I2.** Ainda mais, tal resolução é única módulo $m_1 m_2$.

(3) Enunciado de **I1**. (Podes escrever em português matemático ou usando fórmula mesmo.)

0

Em um determinado planeta m_1, x é equivalente a b_1 e em um planeta m_2 x é equivalente a b_2

(9) Demonstração de **I1**.

se o enunciado dado foi considerado «com gírias», imagine falar de planetas...!

(4) Enunciado de **I2**. (Podes escrever em português matemático ou usando fórmula mesmo.)

0

Existe um único b_1 e um único b_2 tal que ~~$b_1 = b_2 = b$~~ $b_1 \equiv x$ & $b \equiv x$

(8) Demonstração de **I2**.

Só isso mesmo.

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

CONGRUENTES: SÃO IGUAIS.

Não seria muito estranho escrever $x \equiv y \pmod{m}$

Teorema. Seja x inteiro. Para qualquer y inteiro, se isso significasse simplesmente $x = y$?!?

$$x \equiv y \pmod{0} \implies (\forall m \geq 0)\,[x \equiv y \pmod{m}]\,.$$

(6) DEMONSTRAÇÃO.

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$. Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod{n}.$$

Dica: *Não tenha medo aplicar as definições das relações envolvidas.*

DEMONSTRAÇÃO:

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

6

Sejo a, b, m inteiros. Dizemos que a é congruente a b módulo m sse m divide $a-b$.

$$a \equiv_m b \iff m \mid a-b$$

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[x \equiv y \pmod m]\,.$$

(6) DEMONSTRAÇÃO.

(1)

Suponho $x \equiv y \pmod 0$ ✓
sejo m inteiro t.q. $m \geq 0$ ✓
...?

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$. Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: *Não tenha medo aplicar as definições das relações envolvidas.*

DEMONSTRAÇÃO:

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[\,x \equiv y \pmod m\,]\,.$$

(6) DEMONSTRAÇÃO.

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$. Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: *Não tenha medo aplicar as definições das relações envolvidas.*

DEMONSTRAÇÃO:

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

(6)

Sejam a, b, m inteiros.
Def.: a é congruente a b módulo $m \iff m \mid a-b$

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[x \equiv y \pmod m]\,.$$

(6) DEMONSTRAÇÃO.

(5)

Seja y inteiro tq. $0 \mid y-y$. ✓ (logo)
Seja m inteiro tq. $m \geq 0$.
Caso $m=0$:
Imediato pela escolha de y.

Caso $m > 0$:
Testemunho 0.

o que ofereceu essa separação em casos?
onde usou a hipótese do caso $m>0$ mesmo?

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$.
Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: *Não tenha medo aplicar as definições das relações envolvidas.*

DEMONSTRAÇÃO:

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

6

Sejam a,b inteiros. ✓
Seja m inteiro tq $m \geq 0$. ✓
Dizemos que $a \equiv_m b$ (a é congruente a b módulo m), se, somente se, $m \mid a-b$.

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[\,x \equiv y \pmod m\,].$$

(6) DEMONSTRAÇÃO.

6

Seja y inteiro tq $x \equiv_0 y$, ou seja, $0 \mid x-y$. ✓
Logo, seja u tq $0 \cdot u = x-y$. ✓
Temos que, pelo ZM-An, $0 = x-y$. ✓
Logo, seja m inteiro tq $m \geq 0$.
Temos que $m \mid 0$, usando 0 como testemunha. ✓
Logo, $m \mid x-y$, ou seja, $x \equiv_m y$. ✓

→ esse "logo" não faz sentido

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$.
Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: *Não tenha medo aplicar as definições das relações envolvidas.*

DEMONSTRAÇÃO:

:(FALTAVAM 24 MINUTOS!

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO: (bizarro usar nomes maiúsculos)

(3)

$A \equiv B$ (MODULO M) $\iff M \mid A - B$

seco! CADÊ O CONTEXTO?!

Teorema. Seja m inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[\,x \equiv y \pmod m\,]\,.$$

(6) DEMONSTRAÇÃO.

(1)

SEJAM x, y INTEIROS TAIS QUE $x \equiv y \pmod 0$ OU SEJA $0 \mid x - y$

LOGO PARA QUALQUER $m \geq 0$ TEMOS QUE $x \equiv y \pmod m$.

Demonstração por repetição do alvo não funciona.. (sem esta frase estava valendo 2 pts. :( ).

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$. Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: *Não tenha medo aplicar as definições das relações envolvidas.*

DEMONSTRAÇÃO:

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

0

Sejam P, Q e n inteiros tais que dividindo o P e o Q no módulo n ambos os Restos serão 1. ?!

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[x \equiv y \pmod m]\,.$$

(6) DEMONSTRAÇÃO.

0

Seja M int maior igual a 0 → "Seja m≥0."

Calculamos:

$x \equiv_0 y$?

$x \equiv_m y$

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$.
Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: Não tenha medo aplicar as definições das relações envolvidas.

DEMONSTRAÇÃO:

(12) **G**

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) DEFINIÇÃO DE CONGRUÊNCIA MÓDULO UM INTEIRO:

4

CADÊ O CONTEXTO?!

Dizemos que a é congruente a b módulo m se $m \mid a-b$.

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[\,x \equiv y \pmod m\,].$$

(6) DEMONSTRAÇÃO.

4

Suponha $x \equiv y \pmod 0$, (quem é?)	
Logo $x = y$, $[0 \mid x-y]$ (isso não é a justificativa aqui.)	Temos $m \mid x-y$, como $x = y$ (não temos não! Isso é o que queremos demonstrar)
Seja m t.q. $m \geq 0$	Temos $m \mid 0$, ?

aqui necessita ponto final.

(36) **H**

Sejam e, n inteiros tais que $e, \varphi(n)$ coprimos, e seja d inverso de e módulo $\varphi(n)$. Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: *Não tenha medo aplicar as definições das relações envolvidas.*

DEMONSTRAÇÃO: