(72) **D** *Escolhe* ***exatamente duas*** *das* ***D1–D6****.*

(36) **D1.** 1 é positivo. **D2.** Existência e unicidade de mdc. **D3.** $(\equiv_m)$ é uma congruência.

(36) **D4.** Existência e unicidade de inversos na aritmética modular.

(36) **D5.** Não há inteiros x, y tais que $x^2 = 6y^2$. **D6.** a, m coprimos $\implies a^{\varphi m} \equiv_m 1$

Para os D3–D6, os teoremas que demonstramos na disciplina "pré-congruência" são considerados dados. Para os D2–D4, começa tua resposta *enunciando o que tu vai demonstrar.*

DEMONSTRAÇÃO DA D4.

existência $a \equiv_m b \overset{def}{\iff} m \mid a-b$

$(\exists a')[a.a' \equiv_m 1]$

quem é?

$m \mid a.a' \to$

$m \mid a \Rightarrow m = ax + b$

??

unicidade

$(\forall a b c)[a.b \equiv_m 1 \;\&\; a.c \equiv_m 1 \Rightarrow b \equiv_m c]$

DEMONSTRAÇÃO DA D5.

$(\forall x, y : int)[x^2 = 6y^2 \Rightarrow \bot]$

Suponha que existe x t.q. $x^2 = 6y^2$

quem é?

contradição

Só isso mesmo.

(72) **D** *Escolhe* ***exatamente duas*** *das* ***D1–D6****.*

(36) **D1.** 1 é positivo. **D2.** Existência e unicidade de mdc. **D3.** $(\equiv_m)$ é uma congruência.
(36) **D4.** Existência e unicidade de inversos na aritmética modular.
(36) **D5.** Não há inteiros x, y tais que $x^2 = 6y^2$. **D6.** a, m coprimos $\implies a^{\varphi\, m} \equiv_m 1$

Para os D3–D6, os teoremas que demonstramos na disciplina "pré-congruência" são considerados dados. Para os D2–D4, começa tua resposta *enunciando o que tu vai demonstrar.*

DEMONSTRAÇÃO DA D4 . ?

Existencia: ~~$\forall$~~ $(a,m)=1 \Rightarrow (\exists a')[\cancel{a\cdot a' \equiv_m 1}]$. a possui inverso modulo m

Sejam a, m coprimos.

Sejam s, t t.q. $1 \equiv_m sa + tm$. [CL e $(a,m)=1$]

Logo, $sa + t\cdot 0 \equiv_m 1$. [?]

Logo, $sa \equiv_m 1$.

Logo, $as \equiv_m 1$. $= 1$

Escolho s.

Unicidade: ~~$(\forall s,s')[\cancel{a\cdot s \equiv_m 1 \ \& \ a\cdot s' \equiv_m 1 \Rightarrow s \equiv_m s'}]$~~. $(\forall s,s')[\, s, s'$ é inverso de a mod $m \Leftrightarrow s' \equiv_m s]$

Sejam s, s' t.q. ~~$as \equiv_m 1$ & as'~~ são inversos de a modulo m.

Logo, $m \mid as-1$ & $m \mid as'-1$. ← por que cair no nível de (1)?

Logo, $m \mid (as-1) \boxed{+} (as'-1)$. [Combinação Linear]

Logo, ~~$m \mid as-as'$~~ $as-1 \equiv_m as'-1$. (def $\equiv_m$?)

Logo, $as \equiv_m as'$. ~~[Cancelamento inverso modulo m]~~ [

Logo, $s \equiv_m s'$. [como?]

«s» ✓

« um » ✓

DEMONSTRAÇÃO DA D6 .

«t.q. seja» ✗

Seja $R = \{r_1, \dots, r_{\varphi(m)}\}$ $\boxed{\text{t.q. seja}}$ s.r.r. modulo m.

$\boxed{\text{Logo}}$, $aR \equiv a\cdot\{r_1, \dots, r_{\varphi(m)}\}$.

Temos, $aR \equiv_m R$. [?]

Logo, $a\{r_1, \dots, r_{\varphi(m)}\} \equiv_m \{r_1, \dots, r_{\varphi(m)}\}$.

Logo, ~~$a \Rightarrow$~~ $a^{\varphi(m)} \cdot R \cdot R^{-1} \equiv_m R \cdot R^{-1}$. ? ?

Logo, $a^{\varphi(m)} \equiv 1$.

mesma coisa.

usamos o «Logo» para inferir uma prop.

Isso não é uma prop!

Só isso mesmo.

onde usou?!

Fermatinho

(i) $(\forall a)[a^m \equiv_m a]$

Sejam a, m coprimos.

Indução no a.

BASE:

Facil

P.I: $(\forall k)[k^m \equiv_m k \Rightarrow (k+1)^m \equiv_m k+1]$

Seja k t.q. $k^m \equiv_m k$. (HI)

Calculamos:

$(k+1)^m \equiv_m k^m + 1^m$ [S d C]

$\equiv_m k + 1^m$ [HI]

$\equiv_m k + 1$. [$1^n \equiv_m 1$]

(ii). $(\forall a)[a^{m-1} \equiv_m 1]$

Seja a t.q. (a, m coprimos.

Temos $a^m \equiv_m a$.

Logo, seja a' o inverso de a modulo m.

Logo, $(a^{m-1}) \cdot a \equiv_m a$.

Logo, $((a^{m-1}) \cdot a) \cdot a' \equiv_m a \cdot a'$.

Logo, $(a^{m-1}) \cdot (a \cdot a') \equiv_m a \cdot a'$.

Logo, $(a^{m-1}) \cdot 1 \equiv_m 1$

Logo, $a^{m-1} \equiv_m 1$.

(72) **D** *Escolhe **exatamente duas** das **D1–D6**.*

(36) **D1.** 1 é positivo. **D2.** Existência e unicidade de mdc. **D3.** $(\equiv_m)$ é uma congruência.
(36) **D4.** Existência e unicidade de inversos na aritmética modular.
(36) **D5.** Não há inteiros x, y tais que $x^2 = 6y^2$. **D6.** a, m coprimos $\implies a^{\varphi m} \equiv_m 1$

Para os D3–D6, os teoremas que demonstramos na disciplina "pré-congruência" são considerados dados. Para os D2–D4, começa tua resposta *enunciando o que tu vai demonstrar.*

DEMONSTRAÇÃO DA D4 .

(a,m) = 1

donde chegou isso?

$(\forall a, m)[(a,m)=1 \Rightarrow (\exists! a')[a \cdot a' \equiv_m 1]]$

Existência: Sejam $a, m, \boxed{s, t : int}$ t.q. $1 = sa + tm$ -- ALVO: $(\exists a')(\exists x)[mx = aa' = 1]$

Logo $tm = 1 - sa$ $[tm + sa - sa = 1 - sa]$

Logo $-tm = sa - 1$ $[(-1)tm = (-1)(sa-1)]$

Logo $m(-t) = as - 1$ $[(\cdot)\text{-com}]$

Escolho $a' := s$ e $x := (-t)$ como testemunhas

O que aconteceu com as congruências?

Unicidade: -- ALVO: $(\forall a)(\forall a', a'')[a \cdot a' = 1 \ \& \ a \cdot a'' = 1 \Rightarrow a' = a'']$

Sejam a, a', a'' : int t.q. $a \cdot a' = 1$ & $a \cdot a'' = 1$ -- ALVO: $a' = a''$

Logo $a \cdot a' = a \cdot a''$ $[(=)\text{-refl}]$

Logo $(a \cdot a') \cdot a'' = (a \cdot a'') \cdot a''$ [Lemmata 1]

Logo $(a \cdot a'') \cdot a' = (a \cdot a'') \cdot a''$ $[(\cdot)\text{-assoc}, (\cdot)\text{-com}, (\cdot)\text{-ass}]$

Logo $1 a' = 1 a''$ $[(=)\text{-subs}]$

Logo $a' = a''$

DEMONSTRAÇÃO DA D3 .

& $(\equiv_m)$ rel. eq.

$(\equiv_m)$ é uma congruência $\overset{def}{\iff}$ $(\equiv_m)$ é compatível com as operações nos inteiros

- $(\equiv_m)$ é compatível com o $(+)$: $(\forall a, a', b, b')[a \equiv_m a' \ \& \ b \equiv_m b' \Rightarrow a + b \equiv_m a' + b']$

  Sejam a, a', b, b' : int t.q. $a \equiv_m a'$ & $b \equiv_m b'$

  Calc:
  $a + b \equiv_m a' + b'$
  $\equiv_m a' + b'$

  [??]

- $(\equiv_m)$ é compatível com o $(\cdot)$: $(\forall a, a', b, b')[a \equiv_m a' \ \& \ b \equiv_m b' \Rightarrow a \cdot b \equiv_m a' \cdot b']$

  Similar ...

- $(\equiv_m)$ é compatível com o $(-_-)$: $(\forall a, b)[a \equiv_m b \Rightarrow -a \equiv_m -b]$

  Sejam a, b : int t.q. $a \equiv_m b$

  Logo $(-1)a \equiv_m (-1)b$ [Lemmata 1 e se $ax = bx \Rightarrow ax \equiv_m bx$]

  Logo $-a \equiv_m -b$

- $(\equiv_m)$ é compatível com o 0: ()[não precisa ~~fazer~~ demonstrar nada] Só isso mesmo.
- $(\equiv_m)$ é compatível com o 1:

(por quê?)

(plurar)
singular: Lem(m)a

Lemma 1 : $(\forall a, b, x)[\, a = b \Rightarrow ax = bx$

Sejam a, b, x : int t.q. $a = b$

Calc :

$$\begin{aligned} & ax \\ = \; & bx \quad [\text{(=)-Subs } a] \end{aligned}$$

X

(72) **D** *Escolhe **exatamente duas** das **D1–D6**.*

(36) **D1.** 1 é positivo. **D2.** Existência e unicidade de mdc. **D3.** $(\equiv_m)$ é uma congruência.
(36) **D4.** Existência e unicidade de inversos na aritmética modular.
(36) **D5.** Não há inteiros x, y tais que $x^2 = 6y^2$. **D6.** a, m coprimos $\implies a^{\varphi\, m} \equiv_m 1$

Para os D3–D6, os teoremas que demonstramos na disciplina "pré-congruência" são considerados dados. Para os D2–D4, começa tua resposta *enunciando o que tu vai demonstrar.*

DEMONSTRAÇÃO DA D4 .

Existência: $(\forall a,m)[(a,m)=1 \to (\exists x)[a.x \equiv_m 1]]$?

Sejam a, m ints tq $(a,m)=1$ ✓

Como $1=(a,m)$, logo posso escrever 1 como combinação linear de a e m ✓

Logo seja s e t ints tq $as+mt=1$ ✓

Calculamos

$1 = as + mt$

$\equiv_m as + 0.t$ [$\equiv_m$ é compatível com $(\cdot)$]

$\equiv_m as + 0$ [Ann-L]

$\equiv_m as$ [idL-(+)]

Escolho s ✓

Unicidade

$(\forall a,a',a'',m)[a.a' \equiv_m 1 \wedge a.a'' \equiv_m 1 \to a' \equiv_m a'']$

Sejam a, a', a'', m ints tq $a.a' \overset{(1)}{\equiv_m} 1 \wedge a.a'' \overset{(2)}{\equiv_m} 1$

Temos $a.a'' \equiv_m 1$, logo $1 \overset{(1)}{\equiv_m} a.a''$ [pela $\equiv_m$-simetria]

Calculamos:

$a.a' \equiv_m 1$

$\equiv_m a.a''$ [pelo (1)]

Como $a.a' \equiv_m a.a''$ logo $a'.(a.a') \equiv_m a'.(a.a'')$ [pela $\equiv_m$ compatível com $(\cdot)$ (2)]

~~Logo~~

Logo $a'.1 \equiv_m a'.(a.a'')$ [pelo

Logo $a' \equiv_m (a'.a).a''$ [Z(.)-ass]

Logo $a' \equiv_m 1.a''$ [pelo (2)]

Logo $a' \equiv_m a''$ ✓

assim não compila nem em pt.

DEMONSTRAÇÃO DA D3 .

Compatível com as operações $(+),(\cdot),(-),(-)$ & rel.eq.

$(\forall a,a',b,b',m)[a \equiv_m a' \text{ e } b \equiv_m b' \to a+b \equiv_m a'+b']$

Sejam a, a', b, b', m ints tq $a \equiv_m a'$ e $b \equiv_m b'$

pela def de $\equiv_m$ temos que $m \mid a-a'$ e $m \mid b-b'$

Logo sejam k, k' ints tq $mk = a-a'$ e $mk' = b-b'$

Calculamos — cadê a linha?

$(a-a')+(b-b') = mk + mk'$

$= m.(k+k')$

Calculamos

$(a-a')+(b-b') = ((a-a')+b)-b'$

$= ((-a'+a)+b)-b'$

$= -a'+(a+b)-b'$

$= a+b-a'-b'$

$= a+b+(-1)a'+(-1)b'$

$= a+b+(-1)(a'+b')$

$= a+b-(a'+b')$

!!

Calculamos

$mk+k' = (a-a')+(b-b')$

$= a+b-(a'+b')$

Escolho $k+k'$

$(\forall a,a',b,m)[a \equiv_m a' \text{ e } b \equiv_m b' \to a+b \equiv_m a'-b']$

Similar

$(\forall a,b,c)[a \equiv_m b \to ac \equiv_m bc]$

Sejam a, b, c ints tq $a \equiv_m b$

Logo seja k int tq $mk = a-b$

Calculamos

$(mk)c = (a-b).c$

$= ac - bc$

Calculamos

$(mk)c = m(kc)$

Escolho kc

$(\forall a,b,c)[a \equiv_m b \to ca \equiv_m cb]$

Similar

nomes incoisistentes

$(\forall a,a',m)[a \equiv_m a' \to -a \equiv_m -a']$

Sejam a, a', m ints tq $a \equiv_m a'$

Seja k int tq $mk = a-a'$

Calculamos

$-mk = -(a-a')$

$= (-1)(a-a')$

$= (-1)(a+(-1).(-a'))$

$= -a + a'$

$= a'-a$

!!! X

Calculamos

$-mk = m.(-k)$ X

Logo $m(-k) = a'-a$ X

Calculamos

$-a-(-a') = -a+a'$

$= a'-a$

Escolho $(-k)$

Só isso mesmo.

por que cair nesse nível?

não faz sentido ter nenhum desses cálculos nesta demonstração!

(72) **D** *Escolhe* ***exatamente duas*** *das* ***D1–D6****.*

(36) **D1.** 1 é positivo. **D2.** Existência e unicidade de mdc. **D3.** $(\equiv_m)$ é uma congruência.

(36) **D4.** Existência e unicidade de inversos na aritmética modular.

(36) **D5.** Não há inteiros x, y tais que $x^2 = 6y^2$. **D6.** a, m coprimos $\implies a^{\varphi\, m} \equiv_m 1$

Para os D3–D6, os teoremas que demonstramos na disciplina "pré-congruência" são considerados dados. Para os D2–D4, começa tua resposta *enunciando o que tu vai demonstrar.*

DEMONSTRAÇÃO DA D1 .

$(\forall a,b)(\exists d)[d|a \wedge d|b \wedge (\forall c)[c|a \wedge c|b \wedge d|a \wedge d|b \Rightarrow d|c]]$

x??x

sejam a, b.

-- Parte R:

Suponha $(c|a \wedge c|b) \wedge (d|a \wedge d|b)$ (H).

DEMONSTRAÇÃO DA _____ .

Só isso mesmo.

(72) **D** *Escolhe* ***exatamente duas*** *das* ***D1–D6****.*

(36) **D1.** 1 é positivo. **D2.** Existência e unicidade de mdc. **D3.** $(\equiv_m)$ é uma congruência.
(36) **D4.** Existência e unicidade de inversos na aritmética modular.
(36) **D5.** Não há inteiros x, y tais que $x^2 = 6y^2$. **D6.** a, m coprimos $\implies a^{\varphi m} \equiv_m 1$

Para os D3–D6, os teoremas que demonstramos na disciplina "pré-congruência" são considerados dados. Para os D2–D4, começa tua resposta *enunciando o que tu vai demonstrar.*

DEMONSTRAÇÃO DA D3 .

é uma rel. eq.

$(\equiv_m)$ é uma congruência significa que $(\equiv_m)$ é compatível com as operações dos inteiros, e ainda mais $0 \equiv_m 0$ e $1 \equiv_m 1$ pelas propriedades de equivalência (reflexividade, transitividade e simetria). Ou seja, (para $(+)$)

$$(\forall a, a', b, b')[a \equiv_m a' \ \& \ b \equiv_m b' \Rightarrow a + b \equiv_m a' + b']$$

Sejam a, a', b, b': Int tais que $a \equiv_m a'$ & $b \equiv_m b'$.
Calculamos:

$$\begin{aligned} a \equiv_m a' &= a \equiv_m a' + (b + (-b)) \\ &= a \equiv_m a' + b + (-b) \\ &= a + b \equiv_m a' + b \\ &= a + b \equiv_m a' + b'. \end{aligned}$$

isso faz parte do que «compatível com as operações» significa?

?!?

para conseguir essas substituições tu precisa que $(\equiv_m)$ é uma cong. Mas é isso que tu tá tentando demonstrar aqui!

Similar para $(\cdot)$.

e $(-)$?

DEMONSTRAÇÃO DA D4 .

$$(\forall a)(\exists! a')[a a' \equiv_m 1]$$

Existência:

Seja a: Int

Calculamos:

Só isso mesmo.

(72) **D** *Escolhe exatamente duas das D1–D6.*

(36) **D1.** 1 é positivo. **D2.** Existência e unicidade de mdc. **D3.** $(\equiv_m)$ é uma congruência.

(36) **D4.** Existência e unicidade de inversos na aritmética modular.

(36) **D5.** Não há inteiros x, y tais que $x^2 = 6y^2$. **D6.** a, m coprimos $\implies a^{\varphi m} \equiv_m 1$

Para os D3–D6, os teoremas que demonstramos na disciplina "pré-congruência" são considerados dados. Para os D2–D4, começa tua resposta *enunciando o que tu vai demonstrar.*

DEMONSTRAÇÃO DA D4 .

Unicidade ∀

$(\forall a)(\exists a', a'')[a \cdot a' \equiv_m 1$ & $a \cdot a'' \equiv_m 1 \Rightarrow a' \equiv_m a'']$

Sejam a, m coprimos

Calc

$a \cdot a \equiv_m a \cdot a''$

$[\cdot a']$ $a'(a \cdot a') \equiv_m a'(a \cdot a'')$

$[(\cdot)\text{-asso}]$ $(a' \cdot a) \cdot a' \equiv_m (a' \cdot a) \cdot a''$

$1 \cdot a' \equiv_m 1 \cdot a''$

$[(\cdot)\text{ com-}1]$ $a' \cdot 1 \equiv_m a'' \cdot 1$

$[(\cdot)\text{-id-}R]$ $a' \equiv_m a''$

não escrevemos assim justificativas

isso não é um calc.

cadê ele no teu enunciado?

props secas!

∀?

(a, m) coprimos ⇒ a tem inversa modulo m

perdeu acesso ao teu a!

(a, m) coprimo ⇒ $(\forall a)(\exists a')[a \cdot a' \equiv_m 1$ & $1 \equiv_m a \cdot a']$

???

Sejam a, m coprimo

Seja $\boxed{mk}$, t.q. $mk = a \cdot a' - 1$

está declarando um produto?

Calc:

$1 \equiv_m a \cdot a' - \cancel{mk}$

$1 \equiv_m a \cdot a'$

Seja mq. t.q. $mq = 1 - a \cdot a'$

Similar ✗

∎

DEMONSTRAÇÃO DA D1 .

Seja Pos o conjunto dos positivos inteiros

✗ $\boxed{\text{Suponha } 1 \in Pos}$

Pela tricotomia:

$1 = 0$ ou $1 \in Pos$ ou $(-1) \in Pos$

Pegue um elemento m arbitrário de Pos

Pela tricotomia

$m = 0$ ou $m \in Pos$ ou $(-m) \in Pos$

• caso $m \in Pos$ $m > 0$

• caso $(-m) \in Pos$ $-m > 0 > 1$ $= m < 0 < -1$

Portanto, $1 = 0$ é falso (Z-NZero), e que $(-1) \notin Pos$ (1).

$\boxed{\text{Logo } 1 \in Pos.}$

Só isso mesmo.

(72) **D** *Escolhe exatamente duas das D1–D6.*

(36) **D1.** 1 é positivo. **D2.** Existência e unicidade de mdc. **D3.** $(\equiv_m)$ é uma congruência.
(36) **D4.** Existência e unicidade de inversos na aritmética modular.
(36) **D5.** Não há inteiros x, y tais que $x^2 = 6y^2$. **D6.** a, m coprimos $\implies a^{\varphi m} \equiv_m 1$

Para os D3–D6, os teoremas que demonstramos na disciplina "pré-congruência" são considerados dados. Para os D2–D4, começa tua resposta *enunciando o que tu vai demonstrar.*

DEMONSTRAÇÃO DA D1 .

Como 1^2 é positivo $\underbrace{[0 \neq 1;\ (\forall a \neq 0)\ [a^2 \text{ é positivo}]]}_{\text{Lemma}}$

Calculamos

$1^2 = 1 \cdot 1$

$= 1$ [$\mathbb{Z}M$-IdR 1]

Logo 1 é positivo

DEMONSTRAÇÃO DA D6 .

Suponha a, m coprimos

calculamos

$a^{\varphi m} = a^{m-1}$ [propriedade do φ]

$\equiv_m 1$ [fermatinho (II)]

X

o fermatinho é inútil aqui pois não temos m primo.

Só isso mesmo.

Fermatinho (II): a, p coprimos $\Rightarrow a^{p-1} \equiv_p 1$

Suponha a, p coprimos

Seja a' um $(\cdot)$-inverso de a [$\mathbb{Z}$ mod-inv]

como $a^p \equiv_p a$ [Fermatinho (I)]

Logo $a^p \cdot a' \equiv_p a \cdot a'$ [$(\equiv)$ é $(\cdot)$-compatível]

Logo $(a^{p-1} \cdot a) \cdot a' \equiv_p a \cdot a'$ [p é primo, logo $p-1>0$; $a^n = \begin{cases} 1, \text{caso } n=0 \\ a^{n-1} \cdot a, \text{caso } n>0 \end{cases}$]

Logo $a^{p-1} \cdot 1 \equiv_p 1$ [$\mathbb{Z}$M-invR a; $\mathbb{Z}$M-invR a]

Logo $a^{p-1} \equiv_p 1$ [$\mathbb{Z}$M-IdR a^{p-1}]

Fermatinho (I): $a^p \equiv_p a$

Por indução no a

Base

Calculamos

$0^p = 0$ [$a=b \Rightarrow a \equiv b$]

$\equiv_p 0$

por quê?

Passo indutivo

Seja k inteiro t.q. $k^p \equiv_p k$

Calculamos

$(k+1)^p = k^p + 1^p$ [sonho de calouro]

sonho mesmo!

cadê?

$= k^p + 1$

$\equiv_p k^p + 1$ [$a=b \Rightarrow a \equiv b$]

$\equiv_p k+1$ [H.I]

(72) **D** *Escolhe **exatamente duas** das **D1–D6**.*

(36) **D1.** 1 é positivo. **D2.** Existência e unicidade de mdc. **D3.** $(\equiv_m)$ é uma congruência.
(36) **D4.** Existência e unicidade de inversos na aritmética modular.
(36) **D5.** Não há inteiros x, y tais que $x^2 = 6y^2$. **D6.** a, m coprimos $\implies a^{\varphi\, m} \equiv_m 1$

Para os D3–D6, os teoremas que demonstramos na disciplina "pré-congruência" são considerados dados. Para os D2–D4, começa tua resposta *enunciando o que tu vai demonstrar.*

DEMONSTRAÇÃO DA D1 .

Separe em casos a partir da ZP-Tri aplicada em 1.

Caso $1 \neq 0$:

Imediato [$1 \neq 0$].

Caso $1 < 0$:

⋮

Caso $1 > 0$

⋮

DEMONSTRAÇÃO DA D3 .

Seja m : Int.

$(\equiv_m)$ é uma congruência $\iff$ $(\equiv_m)$-refl & $(\equiv_m)$-sym & $(\equiv_m)$-trans & $(+)$-comp & $(\cdot)$-comp & $(-_)$-comp

Vamos demonstrar $(\equiv_m)$-refl:

Seja a : Int.

Calculamos:

$a - a$

$= 0.$

Imediato [(1)-top m].

Vamos demonstrar $(\equiv_m)$-sym:

Sejam a, b : Int t.q. $a \equiv_m b$.

Logo $m \mid b$ & $m \mid a$ [$m \mid a$ & $m \mid b \iff (\forall x, y)[m \mid xa + yb]$].

Logo $m \mid b - a$ [mesmo θ.].

Type error

??

Vamos demonstrar $(\equiv_m)$-trans:

Sejam a, b, c : Int t.q. $a \equiv_m b$ & $b \equiv_m c$.

Logo $m \mid (a-b) + (b-c)$ [$m \mid (a-b)$ & $m \mid (b-c) \Rightarrow (\forall x, y)[m \mid x(a-b) + y(b-c)]$].

calculamos:

$(a-b) + (b-c)$

$= a + ((-b) + (b-c))$

$= a + (((-b) + b) - c)$

$= a + (0 - c)$

$= a - c.$

Só isso mesmo.

(72) **D** *Escolhe exatamente duas das D1–D6.*

(36) **D1.** 1 é positivo. **D2.** Existência e unicidade de mdc. **D3.** $(\equiv_m)$ é uma congruência.

(36) **D4.** Existência e unicidade de inversos na aritmética modular.

(36) **D5.** Não há inteiros x, y tais que $x^2 = 6y^2$. **D6.** a, m coprimos $\implies a^{\varphi m} \equiv_m 1$

Para os D3–D6, os teoremas que demonstramos na disciplina "pré-congruência" são considerados dados. Para os D2–D4, começa tua resposta *enunciando o que tu vai demonstrar.*

DEMONSTRAÇÃO DA D3 .

Parte $(\equiv_m)$ é uma congruência para $(+)$
Seja a, a', b, b' t.q. $a \equiv_m a'$ e $b \equiv_m b'$,
ou seja, $m | a - a'$ e $m | b - b'$
Logo, $m | a - a' + b - b'$ $[m|a \,\&\, m|b \Rightarrow m|a+b]$
Logo, $m | (a+b) - (a'+b')$
Logo, $a + b \equiv_m a' + b'$ ✓

Parte $(\equiv_m)$ é uma congruência para $(\cdot)$
Seja a, a', b, b' t.q. $a \equiv_m a'$ e $b \equiv_m b'$,
ou seja, $m | a - a'$ e $m | b - b'$
Logo, $m | (a - a') \cdot (b - b')$
Logo, $m | a'b' - a'b + ab - ab'$
Logo, $m | a'(b' - b) + a(b - b')$
...e?

Parte $(\equiv_m)$ é uma congruência para $(-)$
Seja a, a' t.q. $a \equiv a'$, ou seja, $m | a - a'$
Logo, $m | -(a - a')$ $[(\forall a, m)[m|a \Rightarrow m|-a]]$
Logo, $m | -a - (-a')$
Logo, $-a \equiv_m -a'$ ✓

Parte $(\equiv_m)$ é uma congruência para 1
Seja $m : \mathrm{Int}$
Logo, $m | 0$ [(1)-Top]
Logo, $m | 1 - 1$
Logo, $1 \equiv_m 1$ ✓

Parte $(\equiv_m)$ é uma congruência para 0
Similar a demonstração para 1

& $(\equiv_m)$ é uma rel. eq.

DEMONSTRAÇÃO DA D2 .

Lemmata?

$(\forall a, b)[(\exists! d)[(d|a \,\&\, d|b) \,\&\, (\forall m \in \mathrm{comdivs}(a,b))[m|d] \,\&\, \underbrace{(\exists s, t)[d = sa + tb]}_{\text{não faz parte do enunciado}}]]$

Seja $a, b : \mathrm{Int}$
Caso $a = 0$ e $b = 0$:
Escolho 0
Logo, $0 | 0$ pela (1)-Top.
Caso contrário:
Seja $C = \{sa + tb \mid s, t \in \mathbb{Z}\}$
~~Vou demonstrar que~~ Como C é $(_-_)$-Fechado pela tricotomia, então $C = \{m\mathbb{Z}\}$
pelo C é $(_-_)$-Fechado $\Rightarrow C = \{m\mathbb{Z}\}$ ✗

??

deveria ser $C = m\mathbb{Z}$
mas quem é m?

Só isso mesmo.

(72) **D** *Escolhe* ***exatamente duas*** *das* ***D1–D6****.*

(36) **D1.** 1 é positivo. **D2.** Existência e unicidade de mdc. **D3.** $(\equiv_m)$ é uma congruência.
(36) **D4.** Existência e unicidade de inversos na aritmética modular.
(36) **D5.** Não há inteiros x, y tais que $x^2 = 6y^2$. **D6.** a, m coprimos $\implies a^{\varphi m} \equiv_m 1$

Para os D3–D6, os teoremas que demonstramos na disciplina "pré-congruência" são considerados dados. Para os D2–D4, começa tua resposta *enunciando o que tu vai demonstrar.*

DEMONSTRAÇÃO DA D4 .

• Existência ?

$(\forall a, m : int)[(a,m)=1 \Rightarrow (\exists a')[a \cdot a' \equiv_m 1]]$

Sejam a e m : int tais que $(a, m) = 1$.

Logo, sejam s e t tais que $1 = sa + tm$. [mdc dos a, b pode ser escrito como comb. lin]

Calculamos: $1 \equiv_m sa + tm$ [pelas escolhas de s, m e pelo $(\equiv_m)$-refl]

$\equiv_m sa + t \cdot 0$ [θ. $m \equiv_m 0$]

$\equiv_m sa$ [$\equiv_m$ é compatível com $(\cdot)$]

Escolho como testemunha o s.

• Unicidade: $(\forall a, a', a'', m)[a \cdot a' \equiv_m 1 \ \& \ a \cdot a'' \equiv_m 1 \Rightarrow a' \equiv_m a'']$

Sejam a, a', a'', m : int tais que $a \cdot a' \equiv_m 1$ & $a \cdot a'' \equiv_m 1$.

Calculamos: $a \cdot a' \equiv_m 1$

$\equiv_m a \cdot a''$ [pela escolha de a'']

Logo $(a \cdot a') \cdot a' \equiv_m (a \cdot a'') \cdot a'$ [$(\cdot)a'$]

Logo $a' \cdot 1 \equiv_m a'' \cdot 1$ [comutatividade e associatividade]

→ Logo $a' \equiv_m a''$ [$(\cdot)$-id]

DEMONSTRAÇÃO DA D6 .

Sejam a, m coprimos. (: int)

definimos como conjunto

Seja o sistema reduzido de resíduos (mod m) $[r_1, r_2 \dots r_{\varphi m}]$ de "length" φm.

O sistema $[ar_1, ar_2 \dots ar_{\varphi m}]$, produzido a partir da multiplicação de a pelos resíduos $r_1, r_2 \dots r_{\varphi m}$ também funciona como sistema reduzido de resíduos (mod m). Como a e m são coprimos e o SRR contém, por definição, todas as congruências possíveis para quaisquer inteiros coprimos com m, os dois sistemas são efetivamente os mesmos (mod m).

o que ofereceu toda essa tinta?

é

• Também por isso, os produtos dos dois sistemas são congruentes (mod m).

$\text{prod}[ar_1, ar_2 \dots ar_{\varphi m}] \equiv_m \text{prod}[r_1, r_2 \dots r_{\varphi m}]$.

Logo $a^{\varphi m} \cdot \text{prod}[r_1, r_2 \dots r_{\varphi(m)}] \equiv_m \text{prod}[r_1, r_2 \dots r_{\varphi m}]$ [pela definição de potência e φm]

Logo $a^{\varphi(m)} \cdot \text{prod}[r_1, r_2 \dots r_{\varphi(m)}] \cdot 1 \equiv_m \text{prod}[r_1, r_2 \dots r_{\varphi(m)}] \cdot 1$ [$_ \cdot 1$]

Logo $a^{\varphi(m)} \equiv_m 1$. [$\equiv_m$ é compatível com a multiplicação e suas regras].

cite o lemma!

o que aconteceu com eles?

Só isso mesmo.

• ($\equiv_m$ é compatível com a multiplicação)

~~$(\forall a, b, x, y, m)\ [a \equiv_m x$~~

$(\forall a, b, x, y, m)\ [a \equiv_m b\ \&\ x \equiv_m y \Rightarrow ax \equiv_m by]$

~~Ou seja, basta demonst~~

Sejam a, b, x, y, m : int tais que $a \equiv_m b$ & $x \equiv_m y$.

Basta demonstrar $m \mid ax - by$.

$$\dfrac{\dfrac{m \mid a-b}{m \mid x(a-b)}\ \text{o. div-mult.} \qquad \dfrac{m \mid x-y}{m \mid b(x-y)}\ \text{o. div-mult.}}{m \mid ax - \cancel{bx} + \cancel{bx} - by}\ \text{o. div-lincomb.}$$

Logo, $m \mid ax - by$ e portanto $ax \equiv_m by$. ✓

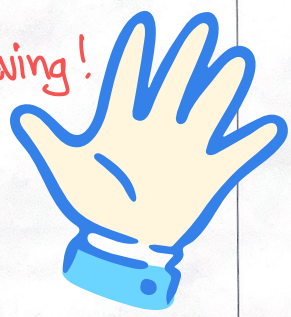
• Vou demonstrar que se um sistema reduzido de resíduos $[r_1 \dots r_{\varphi m}]$ merece o nome de SRR (mod m), um sistema produzido pela map que multiplica os resíduos por um inteiro a coprimo com m também é um SRR (mod m).

TINTA!

$S = [r_1 \dots r_{\varphi m}]$ deve obedecer $(\forall c$ coprimo $m)\ [(\exists r \in S)\ [r \equiv_m c]$. & ...?

Esta propriedade se mantém quando multiplicamos os membros de S por um a coprimo m. Todos os restos possíveis na divisão por m irão manter a congruência dentro do sistema (mod m).

Handwaving!



não escreva texto matemático assim!

(72) **D** *Escolhe* ***exatamente duas*** *das* ***D1–D6****.*

(36) **D1.** 1 é positivo. **D2.** Existência e unicidade de mdc. **D3.** $(\equiv_m)$ é uma congruência.
(36) **D4.** Existência e unicidade de inversos na aritmética modular.
(36) **D5.** Não há inteiros x, y tais que $x^2 = 6y^2$. **D6.** a, m coprimos $\implies a^{\varphi\, m} \equiv_m 1$

Para os D3–D6, os teoremas que demonstramos na disciplina "pré-congruência" são considerados dados. Para os D2–D4, começa tua resposta *enunciando o que tu vai demonstrar.*

DEMONSTRAÇÃO DA D4 .

?

*Existência: $(\forall a, m)[(a, m) = 1 \Rightarrow (\exists a')[a \cdot a' \equiv_m 1]]$

Sejam a, m inteiros coprimos entre si.

Logo, sejam s, t inteiros tais que $sa + tm = 1$. [Lema de Bézout]

Logo, $tm = 1 - sa$.

Logo, $m \mid 1 - sa$. [definição de (1)]

Logo, $1 \equiv_m sa$. [definição de $(\equiv_m)$], logo, $as \equiv_m 1$. [$(\equiv_m)$-simetria] [ZM-Com]

Escolho s como testemunha. ▨

*Unicidade: $(\forall a, a', a'', m)[a \cdot a' \equiv_m 1 \ \&\ a \cdot a'' \equiv_m 1 \Rightarrow a' \equiv_m a'']$

Sejam a, a', a'', m inteiros tais que $a \cdot a' \equiv_m 1$ (1) e $a \cdot a'' \equiv_m 1$ (2).

Calculamos: $a \cdot a' \equiv_m 1$ (1)
$\equiv_m a \cdot a''$ (2)

Logo, $a'(a \cdot a') \equiv_m a'(a \cdot a'')$. [$(\equiv_m)$ é $(\cdot)$-compatível]
Logo, $(a' \cdot a) \cdot a' \equiv_m (a' \cdot a) \cdot a''$. [ZM-Ass]
Logo, $1 \cdot a' \equiv_m 1 \cdot a''$. [(1) e (2)]
Logo, $a' \equiv_m a''$. ▨ [ZM-Id]

DEMONSTRAÇÃO DA D6 .

Sejam a, m coprimos.
Seja $R = \{r_1, r_2, \ldots r_{\varphi m}\}$ um sistema reduzido de resíduos módulo m.
Seja $aR = \{ar_1, ar_2, \ldots, ar_{\varphi m}\}$.
Como, $(\forall r \in R)[(r, m) = 1]$ e $(a, m) = 1$, então $(\forall r \in R)[(ar, m) = 1]$.
~~Logo, aR é um sistema reduzido de resíduos módulo m.~~
Como, $(\forall 0 < i, j \leq \varphi m)[r_i \equiv_m r_j \Rightarrow i = j]$ e $(a, m) = 1$, então $(\forall 0 < i, j \leq \varphi m)$
$[ar_i \equiv ar_j \Rightarrow i = j]$. [como mesmo?]
Logo, aR é um sistema reduzido de resíduos módulo m.
Logo, $ar_1, ar_2, \ldots ar_{\varphi m}$ é uma permutação módulo m dos $r_1, r_2, \ldots, r_{\varphi m}$.
Logo, $ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\varphi m} \equiv_m r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi m}$.
Logo, $a^{\varphi m} \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi m} \equiv_m r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi m}$.
Como $(\forall r \in R)[r$ é invertível módulo $m]$, o produto $r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi m}$ é cancelável.
Logo, $a^{\varphi m} \equiv_m 1$. ▨

Só isso mesmo.

$*$ $(\forall m)[(\equiv_m)$ é $(\cdot)$-compatível$] \iff (\forall m, a, a', b, b')[a \equiv_m a' \;\&\; b \equiv_m b' \Rightarrow ab \equiv_m a'b']$

Seja m inteiro.

Sejam a, a', b, b' inteiros tais que $a \equiv_m a'$ & $b \equiv_m b'$.

~~(Logo, $m \mid a - a'$ e $m \mid b - b'$)~~

~~(Logo, sejam k, j tais que $mk = a - a'$ e $mj = b - b'$)~~

Calculamos: $a \cdot b \equiv_m a \cdot b' \quad [b \equiv_m b']$ ← aqui tá usando o que mesmo?

$\equiv_m a' \cdot b' \quad [a \equiv_m a']$

Logo, $ab \equiv a' \cdot b'$. ∎

(72) **D** *Escolhe* ***exatamente duas*** *das* ***D1–D6****.*

(36) **D1.** 1 é positivo. **D2.** Existência e unicidade de mdc. **D3.** $(\equiv_m)$ é uma congruência.
(36) **D4.** Existência e unicidade de inversos na aritmética modular.
(36) **D5.** Não há inteiros x, y tais que $x^2 = 6y^2$. **D6.** a, m coprimos $\implies a^{\varphi m} \equiv_m 1$

Para os D3–D6, os teoremas que demonstramos na disciplina "pré-congruência" são considerados dados. Para os D2–D4, começa tua resposta *enunciando o que tu vai demonstrar.*

DEMONSTRAÇÃO DA D3 .

cadê?

nomes ruins

~~$(\equiv_m)$ é uma relação de congruência~~

$(\equiv_m)$ é uma congruência $\overset{def}{\iff}$ $(\equiv_m)$ é uma relação de equivalência compatível com as operações.

$(\equiv_m)(+)$ compatível: $(\forall a,a',b)[a \equiv_m a' \Rightarrow a+b \equiv_m a'+b]$

1 arg

Sejam a, a', b t.q. $a \equiv_m a' \overset{def}{\iff} m \mid a-a'$

logo $m \mid a-a'+b-b$

logo $m \mid a+b-(a'+b)$

logo $a+b \equiv_m a'+b$. ■ ✓

por quê?

$(\equiv_m)(-)$ compatível: $(\forall a,b)[a \equiv_m b \Rightarrow -a \equiv_m -b]$

Sejam a, b t.q. $a \equiv_m b$

logo $m \mid a-b$

logo $m \mid -(a-b)$

logo $m \mid -a-(-b)$

logo $-a \equiv_m -b$. ■

2 arg

$(\equiv_m)(\cdot)$ compatível: $(\forall a,a',b,b')[a \equiv_m a' \;\&\; b \equiv_m b' \Rightarrow ab \equiv_m a'b']$

Sejam a, a', b, b' t.q. $a \equiv_m a' \;\&\; b \equiv_m b' \overset{def}{\iff} m \mid a-a' \;\&\; m \mid b-b'$

logo $m \mid (a-a')b + (b-b')a'$. $[x \mid y \;\&\; x \mid z \Rightarrow (\forall s,t)[x \mid ys+zt]$

logo $m \mid ab-a'b' \overset{def}{\iff} ab \equiv_m a'b'$ ■ ✓

DEMONSTRAÇÃO DA D4 .

Existência: $(\forall a, m \text{ coprimos})(\exists a')[a \cdot a' \equiv_m 1]$

Sejam a, m : int t.q. $(a,m)=1$.

logo, sejam s, t : int t.q. $1 = as + mt$. [bezout]

logo $1 = as + 0t$. $[m \equiv_m 0]$

logo $1 = as$.

Escolho s. ■

Unicidade: $(\forall a, a', a'')[aa' \equiv_m 1 \;\&\; aa'' \equiv_m 1 \Rightarrow a' \equiv_m a'']$

Sejam a, a', a'' t.q. $aa' \equiv_m 1 \;\&\; aa'' \equiv_m 1$.

temos $aa' \equiv_m 1$.

logo $aa' \equiv_m aa''$. $[(\equiv_m)\text{-trans}]$

logo $aa' \cdot a'' \equiv_m aa'' \cdot a'$.

logo $(a \cdot a'') \cdot a' \equiv_m (a \cdot a'') \cdot a''$.

logo $1 \cdot a' \equiv_m 1 \cdot a''$.

logo $a' \equiv_m a''$.

■ ✓

Só isso mesmo.

(72) **D** *Escolhe* ***exatamente duas*** *das* ***D1–D6****.*

(36) **D1.** 1 é positivo. **D2.** Existência e unicidade de mdc. **D3.** $(\equiv_m)$ é uma congruência.
(36) **D4.** Existência e unicidade de inversos na aritmética modular.
(36) **D5.** Não há inteiros x, y tais que $x^2 = 6y^2$. **D6.** a, m coprimos $\implies a^{\varphi m} \equiv_m 1$

Para os D3–D6, os teoremas que demonstramos na disciplina "pré-congruência" são considerados dados. Para os D2–D4, começa tua resposta *enunciando o que tu vai demonstrar.*

DEMONSTRAÇÃO DA D4 .

$(\forall a)(\exists! a')[a, a' \in m\mathbb{Z} \Rightarrow a \cdot a' \equiv_m 1]$??

unicidade:

$(\forall a)(\forall a')(\forall a'')[a \cdot a' \equiv_m 1 \ \& \ a \cdot a'' \equiv_m 1 \Rightarrow a' \equiv_m a'']$ Supondo $a \cdot a' \equiv_m 1$ & $a \cdot a'' \equiv_m 1$

calculamos

$a \cdot a' \equiv_m 1$

$a \cdot a' \equiv_m a \cdot a''$ [Refle]

$a' \cdot (a \cdot a') \equiv_m a' \cdot (a \cdot a'')$ ~~[+ cancel]~~ [$\mathbb{Z}_n m$ - canc←]

$(a \cdot a') \cdot a' \equiv_m (a' \cdot a) \cdot a''$ ~~[+]~~ [$\mathbb{Z}_n m$ - ASS]

$(a \cdot a') \cdot a' \equiv_m (a \cdot a') \cdot a''$ [$\mathbb{Z}_n M$ - com]

$1 \cdot a' \equiv_m 1 \cdot a''$ [substituição]

$a' \equiv_m a''$ [$\mathbb{Z}_n M$ - Id]

Existência:

para $a^{-1} = a^{-1}$ tq. a^{-1} é um inverso modulo m de a ??

$a \cdot a^{-1} \equiv_m 1$

DEMONSTRAÇÃO DA D3 .

~~$(\forall m)(\forall a,b)[m \in \mathbb{Z} \ \& \ a,b \in \mathbb{Z} \ \& \ m \mid b - a \Rightarrow b \equiv_m a]$~~

$(\forall m, a, b)[m, a, b \in \mathbb{Z} \ \& \ m \mid b - a \Rightarrow b \equiv_m a]$??

$(\equiv_m)$ é compatível com as operações dos inteiros ✓

$(\equiv_m)$ é reflexivo, simétrico e ?

Só isso mesmo.

(72) **D** *Escolhe* ***exatamente duas*** *das* ***D1–D6****.*

(36) **D1.** 1 é positivo. **D2.** Existência e unicidade de mdc. **D3.** $(\equiv_m)$ é uma congruência.
(36) **D4.** Existência e unicidade de inversos na aritmética modular.
(36) **D5.** Não há inteiros x, y tais que $x^2 = 6y^2$. **D6.** a, m coprimos $\implies a^{\varphi m} \equiv_m 1$

Para os D3–D6, os teoremas que demonstramos na disciplina "pré-congruência" são considerados dados. Para os D2–D4, começa tua resposta *enunciando o que tu vai demonstrar.*

DEMONSTRAÇÃO DA D4 .

Existência ?

a, m coprimos $\Rightarrow (\exists a')[aa' \equiv_m 1]$

Suponha que a coprimo com m.

Logo, $(a, m) = 1$.

Logo, sejam x, y t.q. $ax + my = 1$. [Bezóut]

Cale.:
$$\begin{aligned} 1 &= ax + my \\ &\equiv_m ax + my \\ &\equiv_m ax + 0y \\ &\equiv_m ax + 0 \\ &\equiv_m ax. \end{aligned}$$

Logo, a possui inverso modulo m.

✓

unicidade — onde usou?

$\boxed{a, m \text{ coprimos} \Rightarrow}$ $(\forall a', a'')[aa' \equiv_m 1 \ \& \ aa'' \equiv_m 1 \Rightarrow a' \equiv_m a'']$

Suponha que a coprimo com m.

Sejam a', a'' t.q. $aa' \equiv_m 1$ e $aa'' \equiv_m 1$.

Logo $aa' \equiv_m aa''$.

Logo $a'(aa') \equiv_m a'(aa'')$. [Ø.1]

Logo $(a'a)a' \equiv_m (a'a)a''$.

Logo $(aa')a' \equiv_m (aa')a''$.

Logo $a' \equiv_m a''$.

DEMONSTRAÇÃO DA D6 .

Suponha que a coprimo com m.

Seja $R = \{r_1, r_2, \dots, r_{\varphi(m)}\}$ um s.r.r.

Logo, $aR \equiv_m R$, pois a, m coprimos, ou seja, as posições se trocam. — isso deveria ser um lemma

Logo, $\prod_{i=1}^{\varphi(m)} ar_i \equiv_m \prod_{i=1}^{\varphi(m)} r_i$.

Logo, $a^{\varphi(m)} \cdot \prod_{i=1}^{\varphi(m)} r_i \equiv_m \prod_{i=1}^{\varphi(m)} r_i$.

Logo, $a^{\varphi(m)} \cdot \prod_{i=1}^{\varphi(m)} r_i \equiv_m \prod_{i=1}^{\varphi(m)} r_i \cdot 1$.

Logo, $a^{\varphi(m)} \equiv_m 1$. — O que aconteceu aqui?

Só isso mesmo.

e.1 - $(\forall c, c')[c \equiv_m c' \Rightarrow (\forall a)[ac \equiv_m ac']]$

Sejam c, c' inteiros t.q. $c \equiv_m c'$, ou seja, $m \mid c - c'$. (1)

Seja a int.

Precisamos demonstrar que $m \mid ac - ac' = a(c - c')$.

Como $m \mid c - c'$, (1), logo $m \mid a(c - c')$. [Lemma div-mult].

Logo $ac \equiv_m ac'$.

(72) **D** *Escolhe* ***exatamente duas*** *das* ***D1–D6****.*

(36) **D1.** 1 é positivo. **D2.** Existência e unicidade de mdc. **D3.** $(\equiv_m)$ é uma congruência.
(36) **D4.** Existência e unicidade de inversos na aritmética modular.
(36) **D5.** Não há inteiros x, y tais que $x^2 = 6y^2$. **D6.** a, m coprimos $\implies a^{\varphi\, m} \equiv_m 1$

Para os D3–D6, os teoremas que demonstramos na disciplina "pré-congruência" são considerados dados. Para os D2–D4, começa tua resposta *enunciando o que tu vai demonstrar*.

DEMONSTRAÇÃO DA D4 . ⇐

precisa $(a,m)=1$.

Exist. Inv. mod m:

$(\forall a, m : \text{int})(\exists x)[a \cdot x \equiv_m 1]$

Sejam a, m: int.

Por Bezout, sejam u, v tq. $au + mv = 1$.

Logo $mv = 1 - au$.

Logo $m \mid 1 - au$.

Logo $au \equiv_m 1$.

Escolho u. ∎

Bezout

Unic. Inv. mod m:

$(\forall a, a', a'')[aa' \equiv_m 1 \;\&\; aa'' \equiv_m 1 \Rightarrow a' \equiv_m a'']$

Sejam a, a', a'' tq. $a \cdot a' \equiv_m 1$ e $a \cdot a'' \equiv_m 1$.

Logo $aa' \equiv_m aa''$

Logo $(a \cdot a') \cdot a' \equiv_m (a \cdot a'') \cdot a'$)...

Logo $1 \cdot a' \equiv_m 1 \cdot a''$

Logo $a' \equiv_m a''$ ∎

DEMONSTRAÇÃO DA D3 .

$(\equiv_m)$ é uma congruência $\overset{def}{\Leftrightarrow}$ é compatível com nossa ~~especificação~~ das int: $(+, \cdot, \boxed{-}, -)$.

$(\equiv_m)$ é compatível com $(+)$:

$(\forall a, a', b, b')[a \equiv_m a' \;\&\; b \equiv_m b' \Rightarrow a + b \equiv_m a' + b']$

Sejam a, a', b, b' tq. $a \equiv_m a'$ e $b \equiv_m b'$.

Logo $m \mid a - a'$ e $m \mid b - b'$

Logo $m \mid (a - a') + (b - b')$

Logo $m \mid (a + b) - (a' + b')$

Logo $a + b \equiv_m a' + b'$ ∎

& rel. eq!

Outras operações: SIMILAR (não tanto!)

Só isso mesmo.

(72) **D** *Escolhe* ***exatamente duas*** *das* ***D1–D6****.*

(36) **D1.** 1 é positivo. **D2.** Existência e unicidade de mdc. **D3.** $(\equiv_m)$ é uma congruência.
(36) **D4.** Existência e unicidade de inversos na aritmética modular.
(36) **D5.** Não há inteiros x, y tais que $x^2 = 6y^2$. **D6.** a, m coprimos $\implies a^{\varphi\, m} \equiv_m 1$

Para os D3–D6, os teoremas que demonstramos na disciplina "pré-congruência" são considerados dados. Para os D2–D4, começa tua resposta *enunciando o que tu vai demonstrar.*

DEMONSTRAÇÃO DA D1 .

Vou demonstrar que $1 \in Pos$
Temos $1 \neq 0$ {Z-NZero}
X $\boxed{\text{Sabemos}}$ Tambem que $1 < 0$ É FALSO pois $0 - 1 = -1 \notin Pos$ por quê?
Logo pela {ZP-Tri} Temos $1 > 0$ pois $1 - \overset{=1}{0} \Rightarrow 1 \in Pos$

DEMONSTRAÇÃO DA D5 .

$\neg(\forall x y)[x^2 = 6y^2]$ ALVO: $\perp$
Suponha $(\forall x y)[x^2 = 6y^2]$
Sejam x, y: Ints
Por indução em x^2
Base: $x = 1$
$1^2 = 6y^2$
$1 = 6y^2 \begin{cases} y \geq 1 & 1 = 6 \cdot 1^2 = 1 = 6 \ \times \\ y = 0 & 1 = 6 \cdot 0^2 = 1 = 0 \ \times \ \{NZero\} \\ y < 0 \Rightarrow 1 > 6y^2 & \times \end{cases}$

$\boxed{\text{Não conseguimos demonstrar a base portanto}}$ $(\forall x)[x^2 = 6y^2] = \perp$

XX

Só isso mesmo.

??

(≥) < | > | ≤ |.

1. $x > y \Rightarrow x - y$ pos

2. $x < y \Rightarrow x - y$ Neg

$x \geq y \Rightarrow x > y$ ou $x = y$?

$x \leq y \Rightarrow x < y$ ou $x = y$?