(26) G

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

Um inteiro a que divide um inteiro b tem como resultado um inteiro q mais o resto.

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

Para calcular o mdc de a e b dividimos os dois pelos números primos que dividem os dois e depois os multiplicamos

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) G

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall a,b)(\exists! q,r)[a = bq + r]$ & $0 \leq r < |b|$
$\neq 0$

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$. mdc
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

G1 G2

(a,b) Utilizando Euclides: $a = b \cdot q + r$ $(a,b) = (b,r)$

Se o b direito for 0: o resto for 0 o mdc será o da direita ?? esquerda

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

escrito assim parece que está tentando esconder a idéia

Só isso mesmo.

```
def mdc(a,b):
    if b == 0:
        return b
    else:
        return mdc(b, a%b)
```

(26) **G**

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

Sejam a, b, c : int's, tais que (b.c)

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) **G**

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall d_1, d_2 \neq 0)(\exists q, r)\,[(d_1, d_2) = (q, r)]$ ✗

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) G

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

Sejam a, b, K inteiros, dizemos que a divide b se existe inteiro K tal que $a \cdot K = b$.

isso não é um teorema, mas sim uma definição. (Que tá na primeira página desta prova.)

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO. ??

Sejam o mdc de (a,b) = mdc (b, a) ??
Sejam a, b, q, r : INT
Suponha $a = bq + r$ (⇒) $a - r = bq$
(⇒) não é abrev. para "Logo". Supor essa implicação'
Usando G1; se $(a-r) = b \cdot q$, logo:
logo, $b \mid (a-r) \Rightarrow (\exists q)[b \cdot q = a - r]$

"se"?

O que tudo isso tem a ver com mdc?

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

Para calcular o mdc de dois inteiros a, b, basta dividir ambos a, b pelo maior número em comum presente em seus divisores.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

O que significa "estar presente" num número?

Só isso mesmo.

euclDiv x,y ⇔ (∀x,y)(∃!q,r)[x = qy + r]

(26) **G**

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

euclDiv x y ⇔ y ≠ 0 ⇒ (∃!q,r)[x = qy + r] & ...

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

Seja d = (a,b)
Seja e = (b,r)
Logo d|b e e|b
Seja k tal que dk = b
Seja k' t.q ek' = b

Qual é teu alvo?

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO. — isso não é uma descrição

mdc : Int → Int → Int
mdc _ 0 = 0
mdc 0 _ = 0

mdc _ 1 = 1
mdc 1 _ = 1

mdc x y
|
|
|

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) **G**

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

que notação inventada é essa?

??

b

$(\forall a, b)(\forall q, r)\,(\text{eucdiv}(a,b) = (q,r) / a = b \cdot q + r \;;\; 0 \leq r < a)$

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) **G**

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall a, b)\left[b|a \Rightarrow (\forall r)(\exists q)[a/b = q+r \ \& \ 0 \leq r < |b|]\right]$.

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

$\frac{5}{2} = 2 + 1 \qquad \frac{a}{b} = q + r \qquad a/b = q + r \ \& \ 0 \leq r < |b|$

(26) **G**

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall a, b)(\exists k)[n + k = m,]$.

Quem é?

X

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) G

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

??

quem é

$(\forall a,b:\mathbb{Z})(b\neq 0)(\exists q)(\exists R)\, a/b=K \wedge a-q=R]$ -- a: quociente, R: resto

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) **G**

(6) **G1.** Enuncie o teorema de divisão de Euclides. bugou!
RESPOSTA.

$(\forall a)(\forall b)(\exists q)[a \cdot q = b \Rightarrow (\exists r)\, r \mid a+b\,]$ X

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

Seja $a,b,q,r : INT$ X
Suponha $a = bq+r$ X já feito!
BASTA demons $Com\,div(a,b) = Com\,div(b,r)$ ✓

como demonstramos $(=_?)$ desse tipo?
(Aliás, qual é esse tipo?)

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

USAR EUCDIV PARA CONSEGUIR $\exists r e q$, COM ISSO ADQUIRIR $(a,b)=(b,r)$ E PEGAR OS DIVISORES COMUNS DE UM E ASSIM ADQUIRINDO O DO OUTRO ?? X

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

MDC (a,b) ?
Seja $a,b : INT$
Seja d' t.q $d' \mid a$ & $d' \mid b$ X

Só isso mesmo.

$d = (a,b)$

(26) **G**

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall a,b)(\exists q,r)[a = bq + r]$ & ...
$\neq 0$

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a,b) = (b,r)$. $(r+bq, b) = (a-bq, b)$
DEMONSTRAÇÃO.

--$(a,b) = (b,r)$
Sejam d tq. (a,b) e d' tq. (b,r). TYPE ERROR.
Como $a = bq+r$, então $d = (bq+r, b)$.
Logo, temos $d \mid (bq+r)$ e $d \mid b$.
similarmente, temos $d' \mid a+bq$ e $d' \mid b$. (Qual é teu divo?)
--não sei mais

$a = bq + r$
$(\exists k)[(r+bq+a)k = b]$
$(\exists k')[(r+bq)k' = b]$

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

$b \neq 0$

$(\forall a,b)(\exists! q,r)[a = bq + r \;\&\; 0 \leq r \leq |b|]$

(26) **G**

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA. cadê?

$\neq 0$

$(\forall a,b)(\exists! q,r)[a = bq + r \;\&\; 0 \leq r \leq |b|]$

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

Suponha $0 < r < |b|$. Não quero. (Teu alvo não me obriga.)
Basta: $\text{comDiv}(b,a) = \text{comDiv}(b,r)$. $[(a,b) = (b,a)]$.
Como $a \neq r$ e $r \neq a$. por que trocar??
Imediato. ??

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

top (comDiv (a, b)) ← não é um algoritmo (é uma descrição da definição)

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) **G**

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

~~Para todo m e n inteiros se m divide n então existe K tal que K·m = n.~~
??
X Para qualquer m, n, q e r inteiros, $\frac{m}{n} = nq + r$

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) **G**

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall a)(\forall b \neq 0)(\exists! q, r)[a = b \cdot q + r \ \& \ 0 \leq r < |b|]$

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) G

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall a,b)(\exists! q,r)[b \neq 0 \Rightarrow a = bq + r \ \& \ 0 \leq r < |b|]$

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) **G**

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall a)(\forall b \neq 0)(\exists! q, r)[a = b \cdot q + r \Rightarrow 0 \leq r < |b|]$?

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO. — essa é a def. (Inclusive tá na primeira página desta prova)

sejam m, a, b : Int. m é um m.d.c. dos a, b sse m é um div. comum dos a, b e, para todo c : Int que é um div. com. dos a, b, $c \mid m$.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

$(a, 1) = 1$ ✓ ← não essencial aqui

$(a, 0) = a$ ✗ ← essencial
(↑ 0)

Só isso mesmo.

(26) **G**

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

Se um número primo p divide a.b, p divide a ou b.

Spoiler: (essa vai acabar sendo a def de primo.)

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

- $a = bq + r$
- $(a, b) = (b, r)$

Calculamos:

$b = bq + r$

$b = bq + b$

$b - b = b \cdot q$

$b \cdot q = 0$

↳ ou b é 0, ou q é 0.

CASO $b = 0$

$a = 0 \cdot q + r$

$a = r$

Imediato

CASO $q = 0$.

Similar.

∎

(A def de mdc tá na primeira página.)

?

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

DADOS dois inteiros A e B. ~~Verifique~~ Ache os divisores de A e depois os de B. Mapeie os divisores comuns, se houver. Se há mais de um, ~~verifique~~ ache qual é o que é múltiplo de todos. Esse deverá ser o MDC.

por que separar esse caso?

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

mapear algo a algo é o que uma função faz.

[em?]

Veja bem a def de mdc.

isso parece uma tradução da def.
O que tem a ver com as G1 & G2?

Só isso mesmo.

(26) **G**

(6) **G1.** Enuncie o teorema de divisão de Euclides. (q, r)
RESPOSTA.

Dados dois números naturais n e m, a divisão de euclides recebe eles e retorna o quociente e o resto da divisão entre eles.
eucdiv n m = (n / m, n % m)
↳ função

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

$d \mid a \;\&\; d \mid b \;\&\; (\forall d')[d' \mid a \;\&\; d' \mid b \Rightarrow d' \mid d]$

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) G

definindo? no meio de uma Prop?

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall a, b)\,[a \text{ euclid } b \Leftrightarrow (\exists k, r)[\,b \cdot k \mid (a-r) \wedge a = bk + r\,]]$

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

Busque um número que divida os dois entrados e depois tenha certeza que nenhum outro divisor dos entrados seja capaz de dividilo.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) **G**

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

```
divEuc:: a → b → (c,d)
dE_0 = erro "indefinição"
div n m = (n `div` m , n `rem` m)
```

X

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

Suponha $c \mid a \;\&\; c \mid b$ ✓

$(\exists c)[(c \mid a \;\&\; c \mid b) \Rightarrow (c \mid b \;\&\; c \mid r)]$

↳ o que é isso?

Vou demonstrar $c \mid a \;\&\; c \mid b \Rightarrow c \mid a \Rightarrow c \mid b$

Suponha

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

parece explicação de um código imperativo já escrito.

(6) DESCRIÇÃO.

Caso seja mdc (a,0) a resposta é a, já que a|a e 0 é dividido por todos. Caso contrário, crio uma var cont=1 e um loop que para quando cont ≥ a || cont ≥ b. Se cont divide a e b em resto zero simultaneamente, então multiplico esse resultado do contador pelo resultado dessa mesma função, mas com cont+1

não usamos aspas assim em texto

X

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

parece código funcional

```
mdc :: (a,b) → c
mdc (a,0) = a
mdc (a,b) = calculando 1 (a,b) 0
  where
    calculando cont (x,y) acc
      | cont ≥ x || cont ≥ y = acc
      | otherwise =
        | cont|x && cont|y = calculando (cont+1) (x,y) (acc*cont)
        | otherwise = calculando (cont+1) (x,y) acc
```

2 otherwise?

X

Só isso mesmo.

(26) G

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall a,b)[(\exists! q,r)[b\cdot q+r=a \ \text{e} \ 0\leq r<q]]$
*0 ↳b

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO. "divida x" como se fosse operação unária? X

Divida a recursivamente aplicação 1. Divida b recursivamente aplicação 1. Pegue a lista de divisores comuns até a e b. Pegue o número tal que n top a e n top b

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) G

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall a)(\forall b \neq 0)(\exists! q, r)[a = b \cdot q + r \wedge 0 \leq r < |b|]$ ✓

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) **G**

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall a)(\forall b \neq 0)(\exists! q, r)[a = bq + r \ \& \ 0 \leq r < |b|]$ ✓

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

Seja $d = (b, r)$.
Logo, $d \mid b \ \& \ d \mid r \ \& \ (\forall d')[d' \mid b \ \& \ d' \mid r \Rightarrow d' \mid d]$.
Ou seja 2

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

$mdc(1, a) = (mdc(b, 1) = 1$
??

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Algoritmo:
Dados a e b, app Eucdiv em a b.
Feita a divisão, ~~repita~~
~~repita~~ faça $mdc(b, r)$ até
$b = 1$ ou $r = 1$.

Só isso mesmo.

(26) G

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall a, b : int)\,[b \neq 0 \Rightarrow [(\exists! q, r : int)\,[a = b.q + r \ \& \ 0 \leq r < |b|]]]$ & ...

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

Sejam $a, b, q, r : int$ tais que $a = bq + r$ já feito!
logo $b \mid a$

X

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) G

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

?? tá escrevendo uma def de _|_ ?!

$a/b \overset{\text{def}}{\iff} (\forall a, b \neq 0)(\exists! q, r)[\, q \cdot b + r = a$

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) **G**

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall a)(\forall b \neq 0)(\exists! r, q)[a = bq + r \wedge 0 \leq r < |q|]$

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) G

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

dados x, y inteiros, $y \neq 0$ mdc de x e y

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) G

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

(∀ x y : Nat) [∃ k, r : Nat) [x(-*)(x - ky) ⇔ x/y = ky + r]

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

G 12 ok

(26) **G**

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall a,b,q,r)\,[a=bq+r \Rightarrow \text{Euc.div}_{a,q} = (b,r)\ \&\&\ (0\leq r < b)]$

X

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

$(\forall a,b,q,r)[a=bq+r \Rightarrow (a,b)=(b,r)$
Por indução no b
Caso b=0
$a = 0\cdot q + r$
$= 0 + r$ [(·)Id.1]
$= r$ [(+)Id R]
Imediato
Caso b = Sc
~~Desisto~~

X

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

Cria-se um algoritmo que primeiro verifica se a e b são iguais, ou diferentes.
Caso a=b, o resultado será imediato QUAL?
Caso a≠b, verifica-se qual o menor, e depois o algoritmo sai testando os divisores do menor para ver qual o ~~maior~~ maior divisor comum dos dois.

X

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

(a,b)
Caso a=b
Imediato
Caso a>b
(a,b) = (max d'|b)[d'|a]
Caso b>a
Similar

X

Só isso mesmo.

(26) G

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

Sejam D, d, q, r, tais que o produto entre d e q somado a r equivale a D.

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) G

Cuidado pois pode ser ambíguo: $a \neq 0$ ou não?

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall a, b \neq 0)[(\exists! q, r)[a = b.q + r \wedge 0 \leq r < |b|]]$ ✓

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

Split. → Qual é teu alvo?
Lado L: $(a,b) \mid b$ & $(a,b) \mid r$
Seja d' tal que $d' \mid b \wedge d' \mid r$

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

Divida o número mais pelo menor, se

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) G

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall a)(\forall b \neq 0)(\exists! q, r)[a = bq + r]$ & ...

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) G

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

Verificando em a e b o melhor inteiro c onde c mude tanto a como b.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

?!?!

Só isso mesmo.

(26) G

$0 \leq r < b$

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

PARA DOIS NATS A, B: EXISTE UM Q E UM SÓ R TAIS QUE: $A = B \cdot Q + R$ E $A \geq B > R$

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

SEJAM A, B, Q, R INT. X

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

ENCONTRAR TODOS OS DIVISORES DE A E B, VER OS QUE SÃO DIVISORES DOS DOIS, ESCOLHER O MAIOR DENTRE ELES. X

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

descrição da def.
O que tem a ver com G1 & G2?

Só isso mesmo.

(26) G

?!

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

X

esse teorema fala que para todo a, b, existe um k tal que o mesmo pode resultar em uma divisão entre a e b

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

esse seria o algoritmo, verifica o menor número e armazena o mesmo e subtrai o número ou os dois que foram divididos.

(6) DESCRIÇÃO.

X

```
int a,b;  | if(b > a      | for(int i = 0; i<m; i++)
m = a     | maior=b;}     | { if(a\i!=0 || ...
```

???

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

X

não confunda algoritmo com código

Só isso mesmo.

(26) G

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

EucDiv : (Nat , Nat) → (Nat , Nat) X

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) G

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

$(a, 1) = 1$ e $(a, 0) = a$

desnecessário

essencial ✓

Só isso mesmo.

então

$5 = 5 \cdot 5 + 5$ & $0 \leq 5 < 5$

?

(26) G

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall a, b, q, r : \mathbb{Z})[$ [illegible] $a = b \cdot q + r$ & $0 \leq r < b]$

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

Basta demonstrar que [illegible] $= \mathrm{mdc}(b, r)$

Seja $Y : \mathbb{Z}$ tal que $[\exists K][Y K = a]$ & $[\exists K][Y K = b]$.

Split.

Parte 1:

Imediato por b.

Parte R:

Escolha $K'' := \frac{a}{bq}$.

(1) não dá pra ler

(2) por que traduzir o (1)?

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.

(26) G

(6) **G1.** Enuncie o teorema de divisão de Euclides.
RESPOSTA.

$(\forall a,b)(\exists!q,r)[b\neq 0 \Rightarrow a=bq+r \wedge 0\leq r\leq |b|]$ ✓ :)

(8) **G2.** Sejam a, b, q, r inteiros tais que $a = bq + r$. Demonstre: $(a, b) = (b, r)$.
DEMONSTRAÇÃO.

(12) **G3.** Baseado nos **G1**, **G2**:
descreva **curtamente** um *algoritmo* para calcular o mdc de dois inteiros a, b.
Além da propriedade **G2**, vai precisar mais uma(s?) propriedade(s?) de m.d.c.
Enuncie e demonstre.

(6) DESCRIÇÃO.

(6) ENUNCIADO(S) E DEMONSTRAÇÃO(ÕES).

Só isso mesmo.