(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

$a \equiv_m b \overset{\text{def}}{\iff} m \mid a-b$ -- Def. da congruência módulo. ✓

Vou demonstrar que $(\forall a, b, m, k \in \mathbb{Z})[a \equiv_m b \Rightarrow a+k \equiv_m b]$?!

Sejam a, b, m, k inteiros.

Suponha $a \equiv_m b$.

Logo $m \mid a-b$.

Logo $m \mid a-b+k$. ??

Logo $m \mid a+k-b$.

Por definição de $(\equiv)$, $a+k \equiv_m b$. ∎

Vou demonstrar que $(\forall a, m \in \mathbb{Z})[(a,m)=1 \Rightarrow (\forall b, k \in \mathbb{Z})[ak \equiv_m b \Rightarrow a \equiv_m bk^{-1}]]$

Sejam a, m inteiros

Suponha $(a,m)=1$.

Sejam b, k inteiros.

Suponha $ak \equiv_m b$.

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

Logo $m \mid ak - b$.

Logo $m \mid (ak - b) \cdot k^{-1}$. ← não existe isso nos inteiros

Logo $m \mid a - bk^{-1}$.

Por definição de $(\equiv)$, $a \equiv_m b \cdot k^{-1}$. ■

isso é o $[b]_m$

quem é?

B é s.r.c de $b \overset{def}{\Leftrightarrow} B = \{b' \in B \mid b \equiv_m b'\}$ -- Def. de s.r.c

módulo? B é s.r.r de $b \overset{def}{\Leftrightarrow} B = \{b' \in B \mid b \equiv_m b' \ \& \ (b, b') = 1\}$ -- Def. de s.r.r

Vou demonstrar que $(\forall a, p, m \in \mathbb{Z})[a^{p-1} \equiv_m p \Rightarrow p$ não é primo$]$

Sejam a, p, m inteiros.

... mas $2^{2-1} \equiv_m 2$

Suponha $a^{p-1} \equiv_m p$.

Logo existe k inteiro t.q. $mk + a^{p-1} = p$.

Calculamos:

$mk + a^{p-1} = p$

$a^{p-1}((mk \cdot a^{p-1}) + 1) = p$? ??

Logo $a^{p-1} \mid p$. ■

Só isso mesmo. RIP.

(64) **C**

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

módulo m

TESTAMENTO (1/2)

Congruência: Sejam m, a, b inteiros. Dizemos que a e b são congruentes sse $m \mid a-b$.

o que significa?

0. a invertível módulo $m \iff (a,m)=1$.

Parte ($\Rightarrow$):

Como a invertível mód m logo seja a' tq $aa' \equiv_m 1$. ✓

ou seja, $m \mid aa'-1$. ✓

Logo, seja x t.q. $mx = aa'-1$. ✓

Logo, $mx+1 = aa'$ e logo $1 = aa' + m(-x)$ ✓

Como 1 é uma combinação linear dos a e m. logo $(a,m) \mid 1$ [Bézout] ✓

Logo $(a,m)=1$ [div-ome] ✓

Parte ($\Leftarrow$):

Como $(a,m)=1$ logo sejam x, y t.q. $1 = ax+my$ [Bézout]

Logo $1 \equiv_m ax+my$. e logo $1 \equiv_m ax+0y$ [my multiplo de m]

Logo $1 \equiv ax$ e logo x é um inverso de a módulo m.

tá usando que $(\equiv_n)$ é uma congruência

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

Invertível: Sejam a, m inteiros. Dizemos que a é invertível módulo m, sse existe um a' t.q. $aa' \equiv_m 1$.

Θ. Fermat: $(\forall a)(\forall p \text{ primo})\ [a^p \equiv_p a]$

Sejam a e p t.q. p primo.
Indução no a.
Base: [illegible]:

Calculamos: $1^p = 1$
$\equiv_p 1$

P.I. [illegible]:

Calculamos: $(a+1)^p \equiv_p a^p + 1^p$ [Sonho do calouro]
$\equiv_p a^p + 1$
$\equiv_p a + 1$ [H.I.]

Θ. Sonho do calouro.

...?

Só isso mesmo. RIP.

(64) **C**

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

Não use onde/vírgulas mágicas.

$a \equiv_m b \overset{\text{def}}{\iff} m \mid b-a$, onde a, b, m são inteiros

«Def. Sejam ...
↑ cmd's!

(≡) é uma relação de congruência nos inteiros, ou seja, é uma relação de equivalência e é compatível com as operações da estrutura dos inteiros, e isso é ? "um"? teorema.

Θ. Sejam a, a', m inteiros t.q. $aa' \equiv_m 1$, $(a,m) = 1$:
seja k t.q. $mk = 1 - aa'$, logo $mk + aa' = 1$. Como (m,a) divide todas as combinações lineares dos m, a, logo $(m,a) \mid mk + aa'$, logo $(m,a) \mid 1$, logo $(m,a) = 1$. obs: essa demons foi a menos de sócios.

Θ. A recíproca do teorema acima também "vale". (teria sido escolha melhor)

Θ. Chinês Binário, $(\forall m,n)[(m,n)=1 \Rightarrow (\forall a,b)(\exists x)[x \equiv_m a \text{ e } x \equiv_n b$ e $(\forall x')[x \equiv_{mn} x']]]$. ??? Bizarríssimo "enunciado". Use comandos!!

Sejam m, n inteiros coprimos. Sejam a, b inteiros e sejam também m', n' t.q. $mm' \equiv_n 1$ e $nn' \equiv_m 1$. Testemunhe $ann' + bmm'$.

A parte mais difícil dessa demons já foi feita neste esboço.

Então por que continuar com isso na próxima página??

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

$a nn' + bmm' \equiv_m a$:

Como $m \equiv_m 0$ e $nn' \equiv_m 1$, logo $ann' + bmm' \equiv_m a$, pois $a1 + b0 = a \equiv_m a$.

$ann' + bmm' \equiv_n b$:

Similar.

"Unicidade":

Seja x' tm inteiro t.q. $x' \equiv_m a$ e $x' \equiv_n b$.

Como $x' \equiv_m a$, logo $xx' \equiv_m ax$ Similarmente, $xx' \equiv_m ax'$,

Logo, ~~Como~~ $a' \equiv_m a$, Trivial.

Exercício para o Leitor.

$\blacksquare$

$(\forall a, b, m, n)$

C. $\left[a \equiv_{(m,n)} b \Rightarrow (\exists x)\left[x \equiv_m a \text{ e } x \equiv_n b\right]\right]$

TM

Já tenho demonstrado, apenas faltou tempo.

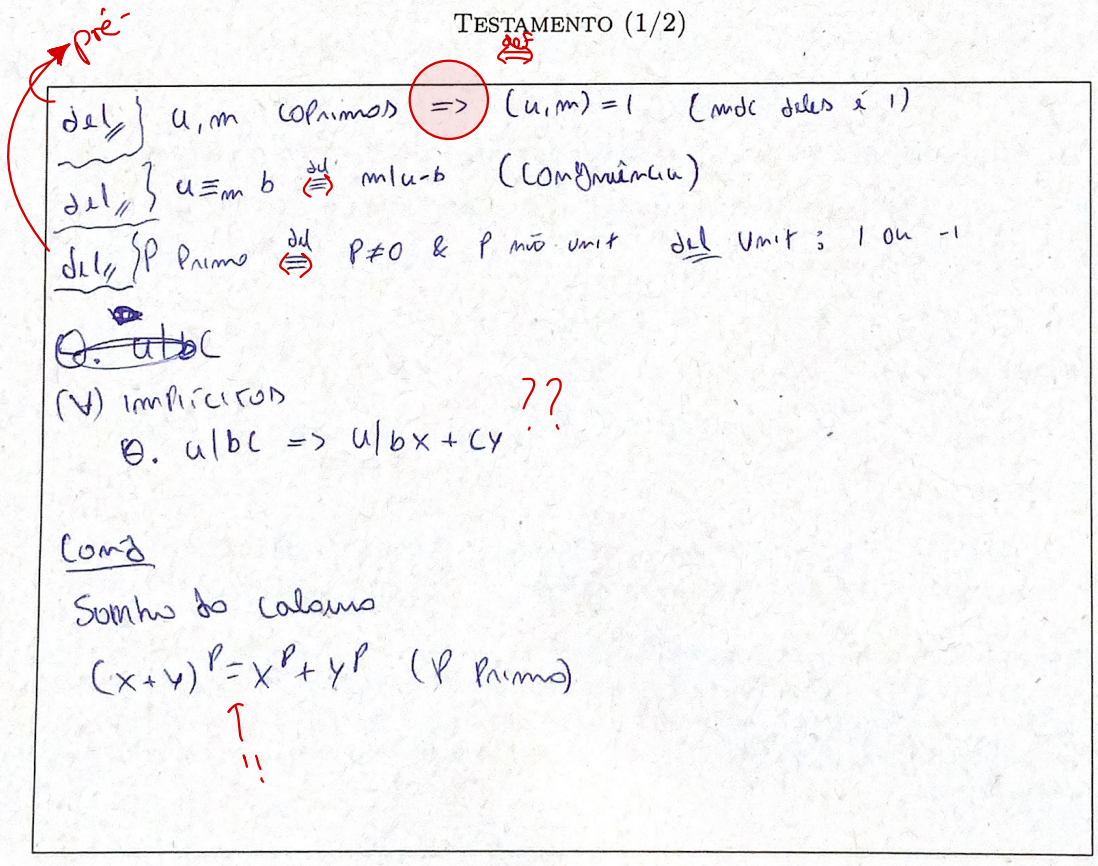
Só isso mesmo. RIP.

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!



[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

u ≡m b ⇔ m | u - b

Θ. $(\forall x, m, x', x'')[\, xx' \equiv_m 1 \;\&\; xx'' \equiv_m 1 \Rightarrow x' \equiv_m x'' \,]$

Suponha $xx' \equiv_m 1$ && $xx'' \equiv_m 1$.

Unicidade dos inversos módulo m

Logo $x'xx' \equiv_m x'xx''$. [$\equiv_m$ é compatível com $\cdot$]

Logo $1.x' \equiv_m 1.x''$.

Logo $x' \equiv_m x''$.

Θ. (Fermat) [redacted] $a^p \equiv_p a$ (p Primo, $a \neq 0$)

Θ. (Fermatinho) $a^{p-1} \equiv_p 1$ (p Primo, $a \neq 0$) a, p coprimos

---

Θ. p Primo $\Leftrightarrow$ p irredutível

pré

Só isso mesmo. RIP.

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

def congruência: a, b, m são o quê?

$a \underset{m}{\equiv} b \overset{\text{def}}{\Leftrightarrow} m \mid a-b.$

A congruência é compatível com (·):

tecnicamente isso é ser compatível com (·x)

$(\forall a,b,x,m)[a \underset{m}{\equiv} b \Rightarrow ax \underset{m}{\equiv} bx]$

Sejam a,b,x,m: Int t. q. $a \underset{m}{\equiv} b$.

Logo $m \mid a-b$.

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

Logo $m \mid xa-bx$. ✓

Logo $ax \underset{m}{\equiv} bx$.

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

Unicidade da compatibilidade com (0): ?!

$(\forall a, b, x, x', m)[\, ax \equiv_m bx' \Rightarrow x \equiv_m x' \,]$ X

Sejam $a, b, x, x', m : \mathbb{Z}$ t.q $ax \equiv_m bx'$.

Logo $m \mid ax - bx'$.

Logo $m \mid x \wedge m \mid x'$.

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

Inversíveis modulo m:

$(\forall a, b, x, m)[$ a,b inversíveis sendo m de x $\Rightarrow$ Esquerda $]$

o que significa isso?

Teoremas que podem ser demonstrados mais facilmente com módulos:

$(\forall a)[a^2 \text{ é par} \Rightarrow a \text{ é par}]$

$(\forall x)[x \text{ é inversível} \Leftrightarrow x \text{ unit}]$

$(\forall x)[3 \mid x^2 \Rightarrow 3 \mid x]$

como isso seria entendível para alguém que nunca viu?

Só isso mesmo. RIP.

(64) **C**

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

Sejam X, Y, m inteiros, X é congruente módulo m se, e somente se, m divide $X-Y$.

$$X \equiv_m Y \overset{\text{def}}{\iff} m \mid X-Y. \quad \checkmark$$

Para $X \equiv_m Y$, Y é um resíduo de X módulo m.

Seja $R = \{r_1, r_2, \ldots r_m\}$. R será um sistema reduzido de resíduos módulo m, se, e somente se:

(i) $(r_i, m) = 1$ para todo $r_i \in R$.

(ii) $r_i \equiv_m r_j \Rightarrow i = j$ (todos os membros de r são disjuntos dois a dois.

(iii) Para todo X, existe $r \in R$ tal que $X \equiv_m Y$. ✓

por que essas defs são úteis?

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

A função totiente de euler, denotado por $\varphi(m)$, sendo m inteiro é definido por:

$$\varphi(m) \stackrel{def}{=} |\{0 < j < m \mid (m, j) = 1\}|$$

$\varphi(1) = ?$

Θ. Teorema de euler: $(\forall a, m)[(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv_m 1]$

Θ*. p primo $\Rightarrow \varphi(p) = p - 1$

Para demonstrar esse teorema, basta mostrar ??
que como $(p, p) \neq 1$ e p é coprimo com todos os j tal que $0 < j < p$, logo $\varphi(p) = p - 1$

Θ. Fermat (p primo $\Rightarrow a^{p-1} \equiv_p 1$)
É corolário fácil do Θ* e do Teorema de Euler.

Só isso mesmo. RIP.

$xx' \equiv_m 1$

(64) **C**

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

Definição de congruência módulo m

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

Notação: $a \equiv b \pmod{m}$ ou $a \equiv_m b$. ✓

A congruência é uma relação de equivalência, ou seja

não é o que ser rel. de equiv. significa.

Teoremas:

(I) $(\forall a, b, c)\,[a \equiv_m b \Rightarrow a \cdot c \equiv_m b \cdot c]$ $(\cdot c)$-compat

(II) $(\forall a, b, c)\,[a \equiv_m b \Rightarrow a + c \equiv_m b + c]$ $(+c)$-compat

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

(III) $(\forall x)(\exists x')[xx' \equiv_m 1 \text{ ou } x'x \equiv_m 1]$? ✗ $(x,m)=1$!

(IV) $(\forall a,b,x)[a \equiv_m b \Rightarrow a^x \equiv_m b^x]$ $(\_^x)$-compat

Sonho de colouro

$(\forall a,b,m)(\exists m)[(a+b)^m \equiv_m a^m + b^m]$

Só isso mesmo. RIP. xx

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2) "" "" ??

Relação de congruência módulo "m":
Def. $(\forall x : Int)(\forall m : Int)[X \equiv_m rem(x, m)]$.

def's não são props!
isso nem compila.
Veja como escrevemos definições.

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

Sejam a, b, m inteiros. Dizemos que $a \equiv_m b$ sse $m | a-b$.
Ou seja: $a \equiv_m b \overset{\text{def}}{\iff} m | a-b$. Temos que $(\equiv_m)$ é uma relação de equivalência. Lemos isso como a é congruente à b módulo m. ~~Mas para ser uma congruência, temos que~~.
Ser uma congruência significa que nossa relação de equivalência é compatível com nossa especificação algébrica dos inteiros. Ou seja, é compatível com $(0, 1, +, (-), \cdot)$
Segue:
~~Ou~~ $(\forall a, b, m, x)[a \equiv_m b \Rightarrow a \cdot x \equiv_m b \cdot x]$.
Sejam a, b, m, x: int t.q $a \equiv_m b$.
Logo $m | a-b$. ~~Logo $m | x(a-b)$~~
Logo $m | x(a-b)$. Logo $m | xa - xb$.
Logo $xa \equiv_m xb$.

Para mostrar que $(\forall a, b, m, x)[a \equiv_m b \Rightarrow a+x \equiv_m b+x]$ é parecido. Fica fácil seguindo a definição. Mesma coisa para

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

mostrar que é compatível com o $(-)$, e com 0 e 1 mais trivial ainda. Uma coisa legal nesse mundo é que se a e m são coprimos, então a tem um inverso módulo m. ✓

① $-(\forall a,m)\,[(a,m)=1 \Rightarrow (\exists x')[ax' \equiv_m 1]]$. ✓

Sejam a, m : int t.q $(a,m)=1$.
Por bizout, sejam s,t : int t.q $as+mt=1$.
Logo $mt = 1-as$.
Logo $m \mid 1-as$. Logo $1 \equiv_m as$. Escolho s. ∎

E ainda mais, esse inverso é único módulo m. ✓

② $(\forall a,m,x',x'')\,[ax' \equiv_m 1 \;\&\; ax'' \equiv_m 1 \Rightarrow x' \equiv_m x'']$

Sejam a, m, x', x'' : Int t.q $ax' \equiv_m 1$ e $ax'' \equiv_m 1$.
Logo $ax' \equiv_m ax''$ [transitividade].
Logo $ax'x' \equiv_m ax''x'$ [compatível com $(\cdot)$]
Logo $1x' \equiv_m 1x''$. Logo $x' \equiv_m x''$.

Deixo como teorema a bicondicional $(a,m)=1 \iff (\exists x')[ax' \equiv_m 1]$. Mais teoremas:

$2 \equiv_2 6 \quad 2 \equiv_4 6 \quad 2 \not\equiv_8 6$

③ $(\forall a,b,m,n)\,[a \equiv_m b \text{ e } a \equiv_n b \iff a \equiv_{mn} b]$.

④ $(\forall a,b,m,n)\,[a \equiv_m b \Rightarrow a^n \equiv_m b^n]$

~~Hm~~. É importante perceber que não podemos tirar conclusões à partir dos expoentes serem congruentes módulo m.

Mais um teorema:

⑤ $(\forall a,b,n,m)\,[(a+b)^n \equiv_m a^n + b^n]$. ✓

:/ ← Euler

Só isso mesmo. RIP.

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

o que significa??

PARA TODO N NATURAL E PARA TODO a E b INTEIROS SE $a \equiv_m b$ (MÓDULO m) LOGO $a^N \equiv b^N$ (MODULO M)

$(\forall N : NAT)(\forall a, b, m)[a \equiv_m b \Rightarrow a^N \equiv_m b^N]$?

SEJA N NAT.

SEJAM a, b, m : INT t.q. $a \equiv_m b$

INDUÇÃO EM N:

~~CASO~~ BASE: $(a^0 \equiv_m b^0)$

COMO $a^0 \equiv_m b^0$ LOGO $1 \equiv_m 1$ X ← esse é teu alvo! X

LOGO $m \mid 1-1$

LOGO $m \mid 0$ ← tu concluiu algo trivial aqui.

IMEDIATO □

PASSO INDUTIVO: $(a^{N+1} \equiv_m b^{N+1})$

COMO $a^{N+1} \equiv_m b^{N+1}$, LOGO $a^N \cdot a \equiv_m b^N \cdot b$ } mesmo problema

LOGO $a^N \equiv_m b^N$ (LEMMA 1)

IMEDIATO [HIPOTESE]

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

$(\forall a, b, c, d, m \in \mathbb{INT})\ [(a \equiv_m b \ \& \ c \equiv_m d) \Rightarrow ac \equiv_m bd]$

SEJAM $a, b, c, d, m \in \mathbb{INT}$ T.Q $a \equiv_m b$ & $c \equiv_m d$

LOGO $m \mid a - b$

LOGO $mk = a - b$ ← quem é k?

LOGO $a = mk + b$

LOGO $(m, b) = a$??

LOGO $a \mid m$ E $a \mid b$ X

COMO $c \equiv_m d$, LOGO $m \mid c - d$

LOGO $mk' = c - d$

LOGO $c = mk' + d$

LOGO $(m, d) = c$

LOGO $c \mid m$ E $c \mid d$

LOGO $ac \mid m$

Só isso mesmo. RIP.

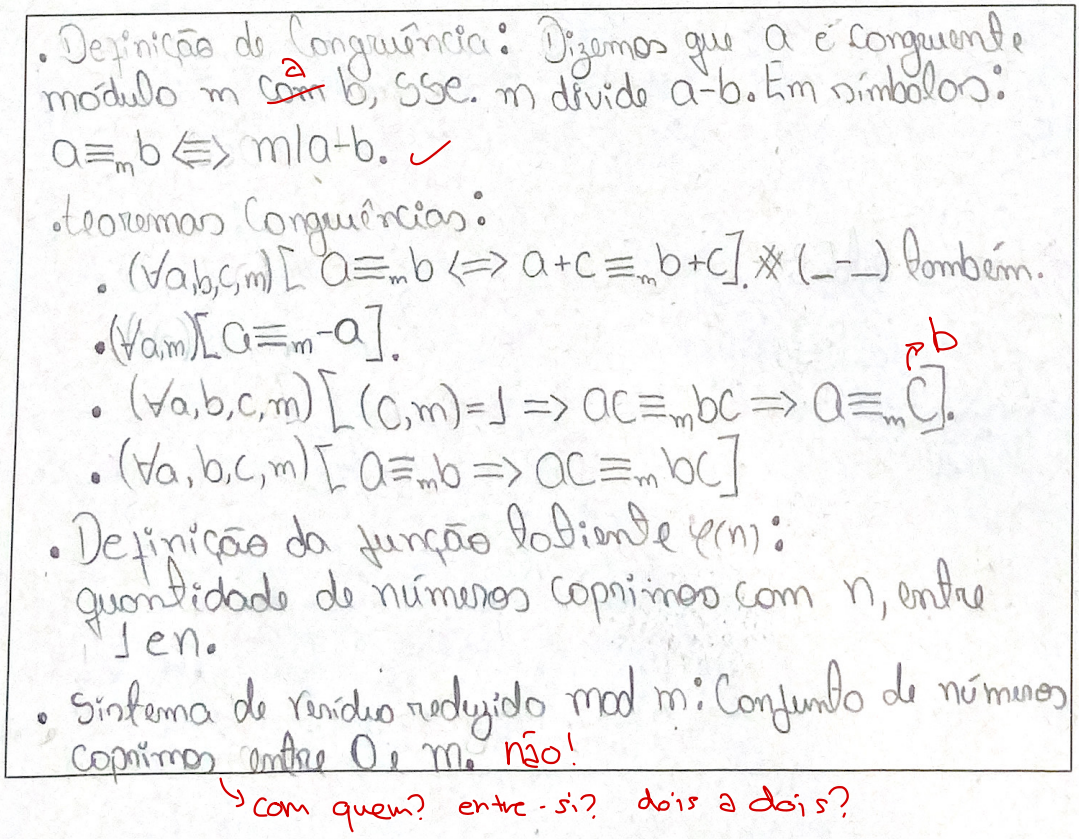
(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)



[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

- Propriedades de $\varphi(n)$:
  - p primo $\Rightarrow \varphi(p) = p-1$. (I)
  - p, q primos $\Rightarrow \varphi(pq) = \varphi(p)\cdot\varphi(q)$. (II)
  - p primo $\Rightarrow \varphi(p^a) = p^a - p^{a-1}$. (III)
    - Rascunho da (III):
      Os números não coprimos com p^a são:
      $1p, 2p, \ldots, p^{a-1}\cdot p$. Ou seja p^{a-1} elementos.
  - teorema bonja: $(\forall a, m)[a^{\varphi(m)} \equiv_m 1]$
  - teorema de Jalezinho: $(\forall a, p)[p \text{ primo} \Rightarrow a^{p-1} \equiv_p 1]$
    - Demonstração:
      Seja a, p t.q. p primo.
      Temos que $p-1 = \varphi(p)$. [Prop. (I)]
      Logo $a^{\varphi(p)} \equiv_p 1$. [Euler] ← decida
  - teorema de Jerê: $(\forall a, p)[p \text{ primo} \Rightarrow a^p \equiv_p a]$
    Seja a, p t.q p primo.
    Temos $a^{p-1} \equiv 1$. [Jalezinho]
    Logo $aa^{p-1} \equiv a$.

Só isso mesmo. RIP.

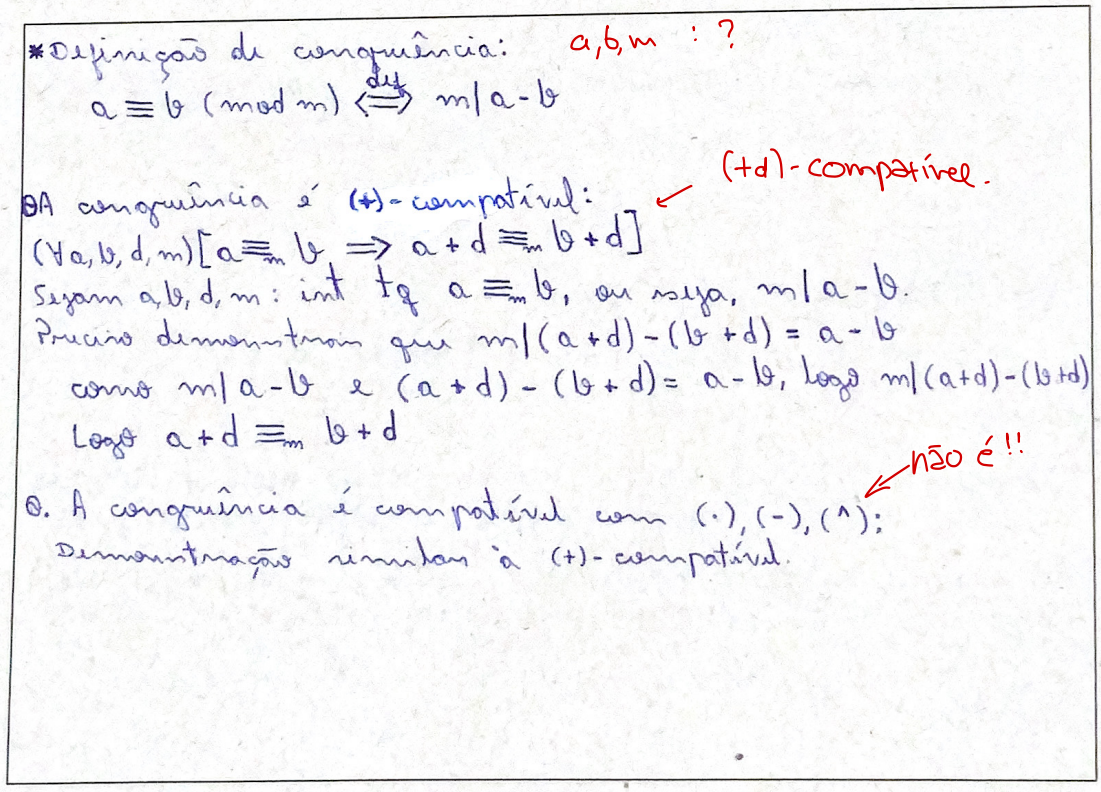
(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)



[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

Q. $(\forall m,n,e,d)[(m,n)=1 \wedge (e,\varphi(n))=1 \wedge ed \equiv 1 \pmod{\cdot}) \Rightarrow (m^e)^d \equiv_n m$?

Sejam m,n,e,d : int tq $(m,n)=1 \wedge (e,\varphi(n)=1 \wedge ed \equiv 1 \pmod{\varphi(n)}$ ✓

Logo $\varphi(n) \mid ed-1$

Logo seja k inteiro tq $k\varphi(n) = ed-1$.

Logo $ed = k\varphi(n) + 1$ (h)

calculamos:

$$\begin{aligned}(m^e)^d &= m^{ed} \\ &= m^{k\varphi(n)+1} \qquad [(h)] \\ &= m \cdot m^{k\varphi(n)} \\ &\equiv_n m \cdot (m^{\varphi(n)})^k \\ &\equiv_n m \cdot 1^k \qquad [??] \\ &\equiv_n m\end{aligned}$$

... mas por que isso seria útil?

Só isso mesmo. RIP.

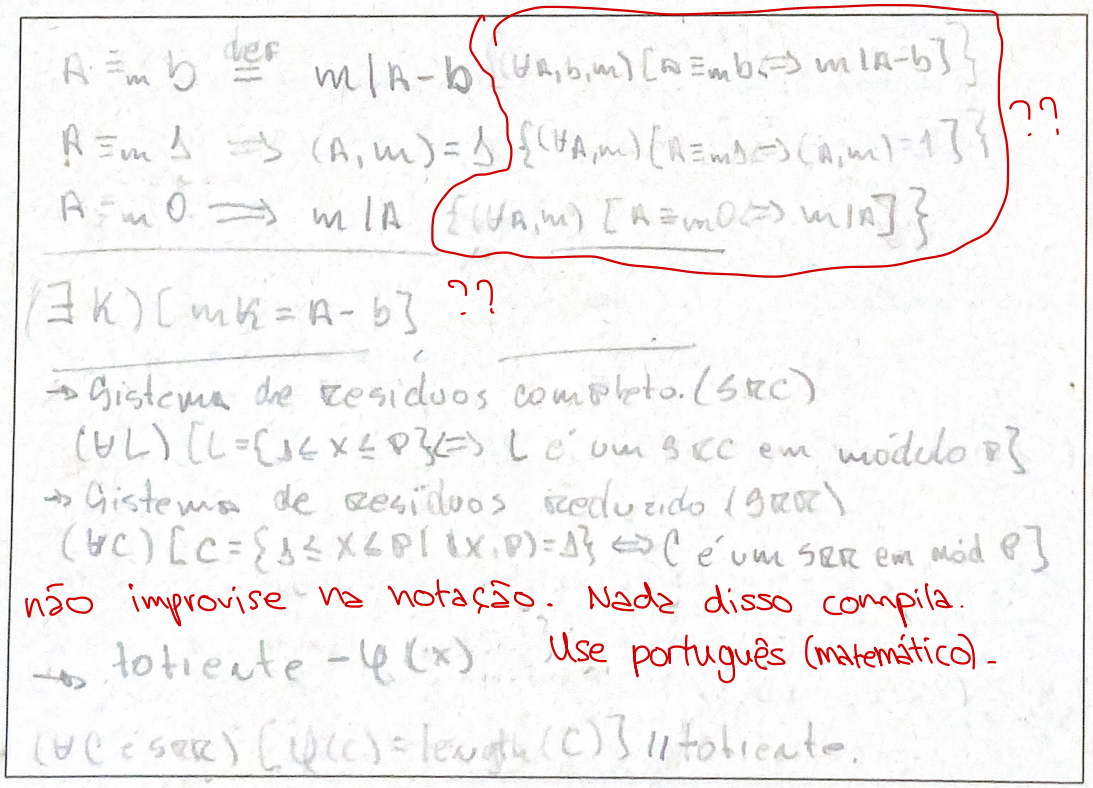
(64) **C**

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)



[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

→ Euler

$A^{\varphi(m)} \equiv_m 1 \iff (A,m)=1$

(⇒)

Suponha $A^{\varphi(m)} \equiv_m 1$ tq ?? $m \mid A^{\varphi(m)}-1$

Seja k, tq $km = A^{\varphi(m)}-1$

Seja $R = \{r_1, \dots, r_p\}$, um set.

(I) Sejam i, j tq $Ar_i \equiv_m Ar_j$

logo, $i = j$. Por quê?

(II) $(A,m)=1$ & $(r,m)=1 \Rightarrow (Ar,m)=1$

(...)

(⇐)

Suponha $(A,m)=1$

[utilizando bezout chegaremos ao alvo] como??

→ teoremas de Fermat

* $(\forall A,p)[A^{p-1} \equiv_p 1]$ (1)

[demonstração usando Euler]

* $(\forall A,p)[A^p \equiv_p A]$

[demonstração usando 1]

Só isso mesmo. RIP.

(64) **C**

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

$_ \equiv _ \pmod{_} : \mathbb{Int} \times \mathbb{Int} \times \mathbb{Int} \to \mathrm{Prop}$ ✓

$a \equiv b \pmod m \stackrel{\text{def}}{=} m \mid a-b$ ✓

Teoremas fáceis:

$(\forall m, a, b, k)\left[a + k \equiv b + k \pmod m \Leftrightarrow a \equiv b \pmod m \right]$ ✓

$(\forall m, a, b, k)\left[a \equiv b \pmod m \Rightarrow a \cdot k \equiv b \cdot k \pmod m \right]$ ✓

$(\forall m, a, b, k)\left[k \neq 0 \Rightarrow a \cdot k \equiv b \cdot k \pmod m \Rightarrow a \equiv b \pmod m \right]$ ✗

$(\forall m)\left[\pmod m \text{ é uma relação de equivalência} \right]$

$(\forall m, a)\left[(m, a) = 1 \Rightarrow (\exists a')\left[a \cdot a' \equiv 1 \pmod m \right] \right]$ ✓

$(\forall m)\left[m \equiv 0 \pmod m \right]$

$(\forall m)\left[m \equiv -m \pmod m \right]$

$(\forall m, a, b)\left[a \equiv b \pmod m \Rightarrow (\forall k)\left[a^k \equiv b^k \pmod m \right] \right]$

Sejam $m, a, b : \mathbb{Int}$ tais que $a \equiv b \pmod m$.
Seja $k : \mathbb{Int}$.
Calculemos:

$a^k \equiv a \cdot a^{(k-1)} \pmod m$ ✗ [não tens $k > 0$ nos dados aqui!]

tu quis dizer $(\equiv_m)$. "$(\mathrm{mod}\ m)$" não é nada.

Nenhuma demonstração?! :-(

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

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

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

Uma notação mais simples (açúcar sintático) é:

$$a \equiv_m b \overset{\text{sug}}{\iff} a \equiv b \pmod{m}.$$

A congruência módulo m goza de certas propriedades:

- Reflexividade: $a \equiv_m a$
- Transitividade: $a \equiv_m b \ \& \ b \equiv_m c \Rightarrow a \equiv_m c$
- Simetria: $a \equiv_m b \iff b \equiv_m a$.

} rel de eq.

Além disso, ela é compatível com a estrutura algébrica dos inteiros. Disso temos, por reflexividade $0 \equiv_m 0$ e $1 \equiv_m 1$.

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

(+). compatível : $(\forall x, y)[a \equiv_m b \ \& \ x \equiv_m y \Rightarrow a+x \equiv_m b+y]$

(.). compatível : Similar

(−). compatível : $a \equiv_m b \Rightarrow -a \equiv_m -b$.

Θ. $(\forall a, p)[(a,p)=1 \ \& \ p \text{ primo} \Rightarrow a^{p-1} \equiv_p 1]$

Θ. $(\forall a, b, p)[p \text{ primo} \Rightarrow (a+b)^p \equiv_p a^p + b^p]$

Def: Dados inteiros a, a' e m, dizemos que a' é inverso módulo m de a sse $a \cdot a' \equiv_m 1$.

Θ. $(a,m) = 1 \Leftrightarrow (\exists a')[a \cdot a' \equiv_m 1]$

Demonstração (esboço):

($\Rightarrow$) Sabemos a, m coprimos. Logo sejam s, t tais que

$1 = as + mt$.

Logo $1 \equiv_m as + mt$

Calc:

$1 \equiv_m as + mt$

$\equiv_m as + 0t$ [Lemma $m \equiv_m 0$]

$\equiv_m as + 0$

$\equiv_m as$

Logo s é inverso de a módulo m.

Só isso mesmo. RIP.

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

pense: por quê isso não faz sentido?

TESTAMENTO (1/2)

- $a \equiv_m b \overset{\text{def}}{\iff} (\forall a,b,m:\text{int})\,[m \mid a-b]$
- $(\forall a,b,c,d,m)\,[a \equiv_m b \;\&\; c \equiv_m d \Rightarrow a+c \equiv_m b+d]$

Demonstração:
Seja a,b,c,d,m inteiros t.q. $a \equiv_m b$ & $c \equiv_m d$
Basta demonstrar $(\exists k:\text{int})\,[mk = (a+c)-(b+d)]$
Calculamos:

$mk = (a+c)-b-d$
$= (mh+b)+(mq+d)-b-d \quad [(\exists h)[a=mh+b]]\;[(\exists q)[c=mq+d]]$
$= mh+mq$
$= m(h+q)$

Escolho $k = h+q$ ■

não tem k no escopo. NÃO compila.

Cuidado: tu nunca usou esses dados!

- $(\forall a,b,c,d,m)\,[a \equiv_m b \;\&\; c \equiv_m d \Rightarrow ac \equiv_m bd]$

Demonstração:

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

Sejam a,b,c,d,m inteiros t.q. $a \equiv_m b$ & $c \equiv_m d$
Basta demonstrar $(\exists k : int)[mk = ac - bd]$
Calculamos:

$$\begin{aligned} mk &= ac - bd \\ &= (mh+b)(mq+d) - bd \quad [(\exists h)[a = mh+b]] \quad [(\exists q)[c = mq+d]] \\ &= mhmq + mhd + mqb + bd - bd \\ &= m(hmq + hd + qb) \end{aligned}$$

Escolho $k = hmq + hd + qb$ ■

- $(\forall a,b,m : int)(\forall n : Nat)[a \equiv_m b \Rightarrow a^n \equiv_m b^n]$

Demonstração
Sejam a,b,m inteiros e n naturais
Suponha $a \equiv_m b$.
Por indução
Caso $n=0$:
Logo $a^0 \equiv_m b^0$
Logo $1 \equiv_m 1$
■ [LEMA ①]

esse é teu alvo! →

esse não é um "caso"!! Esse é teu alvo!

Caso $(\forall k)[a^k \equiv_m b^k \Rightarrow a^{k+1} \equiv_m b^{k+1}]$
Seja k inteiro t.q. $a^k \equiv_m b^k$
Logo $a^k \cdot a \equiv_m b^k \cdot b$ $[a \equiv_m b]$ e...?
Logo $a^{k+1} \equiv_m b^{k+1}$ ■

- $(\forall a,b,m)[a = b \Rightarrow a \equiv_m b]$ (LEMA ①)

Sejam, a,b,m inteiros t.q. $a = b$
Basta demonstrar $(\exists k)[mk = a - b]$
calculamos

$$\begin{aligned} mk &= a - b \\ &= a - a \quad [a = b] \\ &= 0 \end{aligned}$$

Escolho 0 ■

- Fermat: $(\forall p \text{ primo})(\forall a)[a^p \equiv_p a]$
- Fermatinho: $(\forall p \text{ primo})(\forall a)[a^{p-1} \equiv_p 1]$
- $(\forall a,b,c,m)[a \equiv_m b \;\&\; c \equiv_m b \Rightarrow a \equiv_m c]$

Demonstração:
Sejam a,b,c,m inteiros
t.q. $a \equiv_m b$ & $c \equiv_m b$
Basta demonstrar
$(\exists k)[mk = a - c]$
Calculemos

$$\begin{aligned} mk &= a - c \\ &= (mh+b) - (mq+b) \\ &= mh - mq \\ &= m(h-q) \end{aligned}$$

Escolho $k = h - q$ ■

$[(\exists h)[a = mh+b]]$
$[(\exists q)[c = mq+b]]$

Só isso mesmo. RIP.

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

Definição congru '|' ≠ '/'

$a \equiv_m b = m \mid a - b$ a,b,m : ?

Add congru

Para qualquer inteiro a, m, b, a' : $(b+a) \equiv_m (b+a')$ X

Demonstracao

Seja a, m, b, a' inteiros t.q $a \equiv_m a' = m \mid a - a'$?

ID-Cong ? logo $(b+a) \equiv_m (b+a') = a \equiv_m a'$ type error

Para qualquer inteiro a, m, $a \equiv_m a$

Demonstração:

Seja a, m inteiros

Pelo div-Zero, $m \mid 0 = a - a$

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

Mul-congru - Para todo a, a', b, m inteiros, $(ba) \equiv_m (ba')$

Seja a, a', b, m inteiros tq $a \equiv_m a' = m \mid a - a'$

logo $(ba) \equiv_m (ba') \overset{X}{=}{}^{?} m \mid b(a - a')$ [lemma dist-mul]

$= m \mid a - a'$

type error

Zero-congru Para todo a, a', m inteiros, $m \mid a - a' = 0$

Seja a, a', m inteiros tq $m \mid a - a' = 0$

Pelo lemma da dist Zero

Imediato

Só isso mesmo. RIP.

(64) **C**

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

Sejam a,b inteiros. $a \equiv b$ são congruentes modulo m sse $m \mid a-b$. $a \equiv_m b \overset{\text{def}}{\iff} m \mid a-b$.

$(\forall a,m)[a \equiv_m a]$

Sejam a,m : int. Preciso demonstrar que $a \equiv_m a$, ou seja, $m \mid a-a=0$, $m \mid 0$, pois qualquer inteiro divide o 0. ■

$(\forall a,b,c,m)[a \equiv_m b \;\&\; b \equiv_m c \Rightarrow a \equiv_m c]$ → [transitividade]

Sejam a,b,c,m: int. Suponha $a \equiv_m b$ e $b \equiv_m c$, ou seja, $m \mid a-b$ e $m \mid b-c$.

Logo $m \mid (a-b)+(b-c)$. Logo $m \mid a-c$. Logo $a \equiv_m c$. ■

a é inversível modulo $m \overset{\text{def}}{\iff} (\exists a')[aa' \equiv_m 1]$. → [$a'$ é o inverso de a modulo m.]

θ. a é inversível modulo $m \Rightarrow a, m$ coprimos.

Suponha a é inversível modulo m.

Seja a' t. q. $aa' \equiv_m 1$, ou seja, $m \mid aa'-1$.

Logo seja k t. q. $mk = aa'-1$. Logo $aa' + m(-k) = 1$.

Sejam s,t : int t. q. $as + mt = 1$. X?? } bugou aqui.

Escolha $s := a'$ e $t := (-k)$.

■

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

Θ. Unicidade dos inversos.
$(\forall a,u,v)[au \equiv_m 1 \;\&\; av \equiv_m 1 \Rightarrow u \equiv_m v]$
Sejam a,u,v: int t.q. $au \equiv_m 1$ & $av \equiv_m 1$.
Logo $au \equiv_m av$. [Transitividade]
Logo $m \mid au - av = (u-v)a$.
Logo $m \mid u-v$. $[(a,m)=1]$
Logo $u \equiv_m v$.
■

✓

Só isso mesmo. RIP.

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

Definicao de congruência

Sejam a,b,m inteiros. Dizemos que a é congruente a b modulo m se m|a-b

$a \equiv b \pmod m \iff m \mid a-b$ ✓

Propriedades:

$(\forall a,b,x)\ [a \equiv_m b \iff ax + x \equiv_a b + x]$

$(\forall a,b,x)\ [a \equiv_m b \iff ax \equiv_m bx]$

$(\forall a,b,x)\ [a \equiv_m b \Rightarrow a^2 \equiv_m b^2]$

$(\forall a)\ [a \equiv_1 a]$

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

Θ. $(\forall p \text{ primo})[a^{p-1} \equiv_m 1]$

Indução no a

Base

$1^{p-1} \equiv_m 1$

Passo indutivo

Seja l:int tq $l^p \equiv_p l$? mudou o alvo?

Cale:

$(l+1)^p \equiv_p l^p + 1^p$ (por quê?)

$\equiv_p l^p + 1$

$\equiv_p l + 1$

$(\forall m \geq 0)[a \equiv_m b \Rightarrow a \equiv_0 b]$ X

Seja a, b, m:int, t.q $m \geq 0$ e $a \equiv_m b$

ou seja $m \mid a-b$

caso $m = 0$

logo $0 \mid a-b$

caso $m > 0$

logo $m \mid a-b$

} qual o alvo aqui?

(zero divide qualquer inteiro) X não.

Só isso mesmo. RIP.

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

Sejam a, b, m inteiros, dizemos que a é congruente módulo m com b, se e somente se m divide a diferença de a e b.

notação:

$a \equiv_m b$

• É uma relação de equivalência: ✓

$(\forall a, m)[a \equiv_m a]$ Ø. refl

$(\forall a, b, c, m : \text{Int})[a \equiv_m b \wedge b \equiv_m c \Rightarrow a \equiv_m c]$ Ø. sym

$(\forall a, b, m)[a \equiv_m b \Rightarrow b \equiv_m a]$ Ø. trans

• compatibilidade com as operações:

$(\forall a, b, x, m)[a \equiv_m b \Rightarrow a+x \equiv_m b+x]$ Ø. (+) - compatível (+x) - compat

$(\forall a, b, x, m)[a \equiv_m b \Rightarrow ax \equiv_m bx]$ Ø. (·) - compatível (·x) - compat.

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

não é único, mas sim único-módulo-m

TESTAMENTO (2/2)

∅. inversos módulo m.

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

• Definição: totiente.

Seja n um inteiro positivo, o seu totiente é a cardinalidade do conjunto dos números entre 0 e n que são coprimes com n.

Use notação matemática!

$\varphi(n)$ ← que isso??

∅. $(\forall p \text{ primo})[\varphi(p) = p-1]$

∅. $(\forall a, n)[a^{\varphi(n)} \equiv_n 1]$ X $(a,n)=1$

∅. $(\forall a, p)[a^p \equiv_p a]$

[redacted]

Demons $(\forall p \text{ primo})[\varphi(p) = p-1]$:

Seja p [redacted]: Int, t.q. p é primo.

Como p é primo, logo $(\forall 0<a<p)[(p,a)=1]$

Logo $\varphi(p) = p-1$.

Só isso mesmo. RIP.

(64) **C**

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio què *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

Imagine que vivemos em um mundo com uma quantidade limitada de números, ou melhor, não limitado, mas que apenas conseguimos distinguir uma quantidade finita deles. É o critério para diferenciá-los é o resto da divisão euclidiana dele por um certo m. Ou seja, Sejam a, b inteiros, $b \neq 0 \Rightarrow (\exists! q, r)[\, a = bq + r]$ essa frase não faz sentido

Nesse mundo, temos que $x_1 = x_2 \iff$ para um determinado m ele o mesmo resto quando divididos por m. Sendo assim, usamos como notação o $\equiv_m$ para compará-los, e formalizamos da seguinte maneira:

$$a \equiv_m b \overset{\text{def}}{\iff} m \mid b - a$$ essa def é pouco melhor (hw: por quê?)

E dizemos que "a é congruente módulo m à b" ✓

Para essa relação temos algumas propriedades: $(\forall a, b, c, m : \text{Int})$

- Reflexividade: $a \equiv_m a$
- Transitividade: $(a \equiv_m b \;\&\; b \equiv_m c) \Rightarrow a \equiv_m c$
- Simetria: $a \equiv_m b \iff b \equiv_m a$ ✓

Também temos alguns teoremas: Considere os $\forall$ implícitos

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

Θ. $(a, m) = 1 \Leftrightarrow (\exists a')[a a' \equiv_m 1]$

Esboço: Parte $\Rightarrow$ invoque os coefs. de Bézout, abra a definição e (ZA-Pass)
Parte $\Leftarrow$ Faça de trás pra frente e lembre que (a,b) divide quaisquer combinações lineares de a,b t.q ela é igual ao (a,b)

Θ. $a \equiv_m b \Leftrightarrow a + x \equiv_m b + x$

Esboço: Parte $\Rightarrow$ abra a definição e use (ZA-Inv) no x
Parte $\Leftarrow$ abra a definição e comute os termos pra usar (ZA-Inv)

Θ. $a \equiv_m b \Rightarrow ax \equiv_m bx$

Esboço: Ao abrir a definição use (Z-Distr) e perceba que só vai aumentar o quociente de algo que você já tem

E segue mais alguns que meu tempo de vida restante me impede de demonstrar mas acredito no teu potencial.

Θ. $((c, m) = 1 \;\&\; ac \equiv_m bc) \Rightarrow a \equiv_m b$

Θ. $x^2 + y^2 \equiv_m (x + y^2)$

Θ. $(\forall 0 \leq a < p)[a^p \equiv_p a]$

Esboçou as mais fáceis dando dicas mas nem esboço para as mais interessantes..

:(← Euler

Só isso mesmo. RIP.

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

nem sabemos o que são essas coisas

No meu sonho a congruência e aritmética modular gozam dessas propriedades.

- Definição de congruência.

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

  - Ela ~~também~~ é compatível com alguns elementos da nossa especificação dos inteiros: ✓
    - Compatível com o $0, 1, (+), (-), (\cdot)$.

- Alguns teoremas.

  $(\forall a, m)[(a, m) = 1 \iff (\exists a')[aa' \equiv_m 1]]$

Esboço: ← nem esboço foi, foi demonstração pera qual
Parte ($\Rightarrow$): gastou metade de folha!

não...

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

Sejam s,t t.q. $as + mt = 1$

Logo $-mt = as - 1$.

Logo $m \mid as - 1$.

Logo $as \equiv_m 1$.

Parte ($\Leftarrow$):

Logo $m \mid aa' - 1$.

Logo sexa k t.q. $mk = aa' - 1$

Logo $mk - aa' = 1$.

Logo $(a,m) \mid 1$.

Logo $(a,m) = 1$. □

- Sistema de resíduos de um a:
  - Completo: $s.c.r. = \{x \mid 0 \leq x \leq a\}$?!
  - Reduzido: $s.r.r. = \{x \mid 0 \leq x \leq a \;\&\; x \neq_a 0\}$.
- Totiente de Euler: $\varphi(n) = |s.r.r.|$ ← s.r.r. não é um conjunto
  - P primo $\Rightarrow \varphi(P) = P - 1$

    Esboço:

    Note que se p primo, para qualquer $0 < a < P$, a é coprimo com P. Logo, existem $P-1$ coprimos entre 0 e P. Logo, $\varphi(P) = P - 1$.
  - $(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv_m 1$.
- Fermat: ??
  - $(\forall a)(\forall P \text{ primo})[(a,P) = 1 \Rightarrow a^{P-1} \equiv_P 1]$

  Ebosço:

  Por Euler, $a^{\varphi(P)} \equiv_P 1$.

  Logo $a^{P-1} \equiv_P 1$.

que isso?

Só isso mesmo. RIP.

$(\forall a,b,x,x')\ [\ x \equiv_{m_1} a \wedge x \equiv_{m_2} b \wedge x' \equiv_{m_1} a \wedge x' \equiv_{m_2} b \Rightarrow x = x'\ ]$

(64) **C**

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

~~Primeiramente, precisamos definir congruência. Sejam a, b inteiros se e só se, a é congruente a b módulo m se e somente se $m \mid a-b$.~~

Definição: Seja a, b inteiros. a é congruente a b módulo m se e somente se $m \mid a-b$. ✓

?

Teorema: Todo sistema de congruencia tem resolução e é unica

$(\forall a,b)(\exists x)[\ x \equiv_m a \wedge x \equiv_{m_2} b\ ]$

Unicidade: ~~$(\forall a,b,m_1,m_2)$~~ $(\forall a,b,x,x')\ [x \equiv_{m_1} a \wedge x \equiv_{m_2} b \wedge x' \equiv_{m_1} a \wedge x' \equiv_{m_2} b$

$\Rightarrow x = x'\ ]$??

Definição: Sejam a, b inteiros. a e b são coprimos se $(a,b) = 1$ (conhecido!)

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

Teorema: $(\forall a, a')\,[a \cdot a' \equiv_m 1 \Leftrightarrow (a, m) = 1]$ - Teorema legal

Teorema: $(\forall a, b)\,[aX \equiv_m bX \Rightarrow a \equiv_m b]$

Teorema: ~~$(\forall a)(\forall p \text{ primo})$~~ $(\forall a)\,[a^{p-1} \equiv_m a^p]$ - Fermat

Teorema: $(\forall a, b)\,[(a+b)^n \equiv_m a^n + b^n]$ - Sonho de calouro

Teorema de Euler ?

Teorema chinês do resto ?

demonstração:

Teorema Legal:

Sejam a, a' int.

Parte ($\Rightarrow$)

Suponha $a \cdot a' \equiv_m 1$

~~logo~~ $m \mid 1 - aa'$

Seja k t.q $mk = 1 - aa'$

logo $mk + aa' = 1$

logo mdc = 1 (Lemma de Bézout)

Parte ($\Leftarrow$)

Suponha $(a, m) = 1$

~~logo~~ Seja u, v t.q $au + mv = 1$

Unicidade das resoluções

Sejam a, b, x, x' inteiros t.q

$x \equiv_{m1} a \wedge x \equiv_{m2} b \wedge x' \equiv_{m1} a \wedge x' \equiv_{m2} b$

Logo

acabou o tempo :(

∴

Só isso mesmo. RIP.

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

Vou introduzir a relação de congruência, ela é uma relação de equivalência e compatível com (+) e (·).

$a \equiv_m b$ significa a congruente b módulo m

$a \equiv_m b \overset{\text{def}}{\iff} m \mid (a-b)$

a invertível módulo $m \overset{\text{def}}{\iff} (\exists a')[a \cdot a' \equiv_m 1]$

Θ. $(a, m) = 1 \iff$ a invertível módulo m

~~Parte (⇐).~~

Θ. $(a, mn) = 1 \iff (a, m) = 1 \;\&\; (a, n) = 1$ conhecido

Parte (⇒):

Sejam u, v : Int t.q. $au + mnv = 1$. [Bezout]

Logo $(a, m) = 1$. [Bezout]

Logo $(a, n) = 1$. [Bezout]

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse*.

Parte (<=):

Sejam u, v : Int t. q. $a \cdot u + m \cdot v = 1$. [Bezout]

Sejam u', v' : Int t. q. $a \cdot u' + m \cdot v' = 1$. [Bezout]

Logo $a(a \cdot u \cdot u' + u \cdot m \cdot v') + m(v \cdot a \cdot u' + v \cdot m \cdot v') = au + mv$.

Logo $(a, m) = 1$. [Bezout]

■

Q. P Primo $\Rightarrow (x+y)^P \equiv_P x^P + y^P$

Q. P Primo $\Rightarrow (\forall 0 \leq a < P)\ [a^P \equiv_P a]$

$\Psi(n) \overset{def}{=} |\{x \mid 1 \leq x < n \ \&\ (x, n) = 1\}|$

Q. $P \overset{>0}{\text{Primo}} \Rightarrow \Psi(P) = P - 1$

~~Seja P ...~~

Q. $n > 2 \Rightarrow \Psi(n)$ Par

Só isso mesmo. RIP.

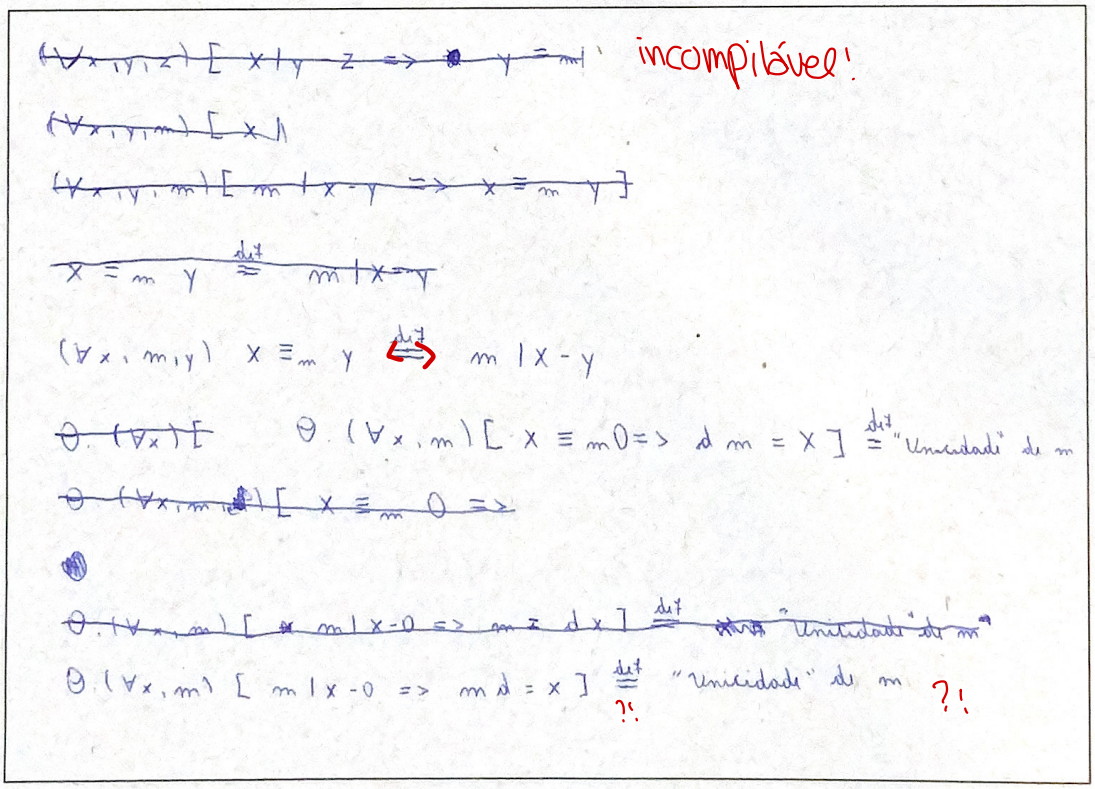
(64) **C**

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)



[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

$a \equiv_m b \overset{def}{\Leftrightarrow} m \mid a-b \overset{def}{\Leftrightarrow} a \equiv b \pmod m$

0. $a \equiv_m b \;\&\; b \equiv_m c \Rightarrow a \equiv_m c$

Demonst:

Sejam $a \equiv_m b$ & $b \equiv_m c$ t.q $a \equiv_m c$

ou seja $m \mid a-b$ & $m \mid b-c$

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

Logo $m \mid (a-b+b)+(-c)$ [(ZA-Ass) $a:=a-b$, $b:=b$, $c:=-c$]

Logo $m \mid (a+b-b)+(-c)$ [(ZA-Com) $a:=b$, $b:=b$]

Logo $m \mid (a+0)+(-c)$ [(ZA-InvR) $a:=b$, $-a:=-b$]

Logo $m \mid a-c$

∎

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

⊖. Seja p primo, $a^p \equiv_p a$

⊖. $a \equiv_m b \Rightarrow b \equiv_m a$

a inversível (mod m) $\stackrel{def}{=}$ $a \cdot a^{-1} \equiv_m 1$?

R é o sistema de resíduos completos $\stackrel{def}{=}$ $[a \equiv_m x \mid x \in R]$

?

Só isso mesmo. RIP.

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

Definição congruência:
Sejam a, b, m inteiros. Dizemos que a é congruente ao b módulo m se, e somente se, $m \mid a-b$.

Definição s.r.r:
Seja $R = \{r_1, r_2 \cdots r_{m-1}\}$. Dizemos que R é um sistema reduzido de resíduos módulo m se

$(\forall m, i, j)[ar_i \equiv_m ar_j \Rightarrow i = j]$ & ...

A ideia seria não precisar disso mais.

~~0.~~ $(\forall x)[x^2 \text{ par} \Rightarrow x \text{ par}]$.

Seja x tal que x^2 é par, ou seja, $x^2 \equiv_2 0$.

Ao dividir x por 2 pela Euc-Div, temos q, r tais que $x = 2q + r$ e $0 \leq r < 2$.

Como $x \equiv_2 1$:

logo $x^2 \equiv_2 1$.

Contradição $[x^2 \equiv_2 0]$.

logo $x \equiv_2 0$, ou seja, x é par.

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

$\theta.\ (\forall a,m)[(a,m)=1 \Rightarrow a^{\varphi(m)} \equiv_m 1]$ -- Teorema 2.

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

Vou demonstrar $(\forall m,i,j)[an_i \equiv_m an_j \Rightarrow i=j]$. r_i? r_j?

Seja $R=\{n_1, n_2 \dots n_{\varphi(m)}\}$ um s.n.n módulo m.

Sejam m, i, j tais que $an_i \equiv_m an_j$.

Logo $n_i \equiv_m n_j$.

Logo $i=j$ [R é um s.n.n mod m].

Como $(n,m)=1$ e $(a,m)=1$, logo $(an,m)=1$ e logo todos os membros de aR são coprimos com m.

Logo $an_1 \cdot an_2 \cdots an_{\varphi(m)} \equiv_m n_1 \cdot n_2 \cdots n_{\varphi(m)}$. por quê?

Logo $a^{\varphi(m)} \cdot (n_1 \cdot n_2 \cdots n_{\varphi(m)}) \equiv_m n_1 \cdot n_2 \cdots n_{\varphi(m)}$.

Logo $a^{\varphi(m)} \equiv_m 1$ [são concebíveis mod m por serem todos coprimos com m].

~~(∀e,d,m)~~ $(\forall e,d,m)[ed \equiv_{\varphi(m)} 1 \Rightarrow (m^e)^d \equiv_m m]$.

Sejam e, d tal q $ed \equiv_{\varphi(m)} 1$, ou seja, $\varphi(m) \mid ed-1$

Logo seja k t.q $k\varphi(m) = ed-1$, ou seja, $ed = k\varphi(m)+1$. (H)

Calc.:

$(m^e)^d \equiv_m m^{ed}$

$\equiv_m m^{k\varphi(m)+1}$ [H]

$\equiv_m m \cdot m^{k\varphi(m)}$

$\equiv_m m \cdot 1^k$ [Pelo Teorema 2] ...e?

$\equiv_m m \cdot 1$

$\equiv_m m$

Só isso mesmo. RIP.

(64) **C**

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

Sejam a, b, m inteiros. Dizemos que a é congruente com b modulo m s.s.e $m \mid a-b$. Em símbolos:

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

$(\equiv_m)$ é compatível com

Para qualquer m em $(\equiv_m)$, as operações $(+), (-), (\cdot)$ são válidas. demonstração:

Sejam a, a', b, b' tal que $a \equiv_m a'$ e $b \equiv_m b'$, logo $m \mid b-b'$ e $m \mid a-a'$, logo $m \mid (b-b')+(a-a')$.

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

Pela definição de congruência, $a+b \equiv_m a'+b'$.

As outras operações são similar.

definição: A congruência é transitiva ($a \equiv_m b$ e $b \equiv_m c \Rightarrow a \equiv_m c$) reflexiva ($a \equiv_m b \iff b \equiv_m a$) e simétrica ($a \equiv_m a$).

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

Considere $\varphi(x)$ a cardinalidade de x a partir do totiente de euler. O que é isso??

Teorema:
Para a, m coprimos, temos
$a^{\varphi(m)} \equiv_m 1$

demonstração:
Temos $(a,m)=1$.
Seja $R=\{r_1, r_2, \dots, r_{\varphi(m)}\}$ um s.r.r(*) módulo m. ✓
Seja $aR=\{ar \mid r \in R\}$ ✓
Como $(a,m)=1$ e $(r,m)=1$, logo $(ar,m)=1$. ✓
Logo, se $ar_i \equiv_m ar_j$, então $r_i \equiv_m r_j$. [?]
Como R é s.r.r, logo $i=j$.
Logo: $\prod_{i=1}^{\varphi(m)} r_{(i)} \equiv_m \prod_{i=1}^{\varphi(m)} ar_{(i)} \equiv_m a^{\varphi(m)} \prod_{i=1}^{\varphi(m)} r_{(i)}$ (porque?)
Logo $1 \equiv_m a^{\varphi(m)}$
■

definição: dizemos que a inversível módulo m sse existir a' tal que $aa' \equiv_m 1$, e $(a,m)=1$

Teorema: $(\exists a')[aa' \equiv_m 1] \Leftrightarrow (a,m)=1$

demonstração:
($\Leftarrow$)
Suponha $(a,m)=1$.
Por Bézout, sejam s,t int. tq $as+mt=1$.
Logo $mt=1-as$.
logo $m \mid 1-as$.
logo $1 \equiv_m as$ (pela def. de congruência)
Escolho s como a'.
logo $aa' \equiv_m 1$.
($\Rightarrow$)
Suponha $(\exists a')[aa' \equiv_m 1]$.
Seja a' tal que $aa' \equiv_m 1$.
Logo $m \mid 1-aa'$.
Logo seja k tq $mk=1-aa'$.
Logo $1=mk+aa'$.
Logo $(a,m) \mid 1$. $[[\text{bézout}]^{s:=a'}_{t:=k}]$
Logo $(a,m)=1$.
■ ✓

definição: Para qualquer modulo m, todo a é congruente de si mesmo.

teorema: $a \equiv_m a$

demonstração:
Temos que $m \mid 0$ pois $0=0m$, sendo $0=k$. X — quem é k?
Como $0=a-a$, logo $m \mid a-a$.
Pela definição de congruência $a \equiv_m a$.

(*) s.r.r = sistema reduzido de resíduos.

Só isso mesmo. RIP.

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

(definição)

Sejam a, b, m inteiros. a é congruente ao b módulo m, se e somente se, $m \mid a-b$.

Em símbolos: $a \equiv_m b \iff m \mid a-b$. ✓

(teoremas)

① $(\forall x, x', y, y')[x \equiv_m x' \;\&\; y \equiv_m y' \Rightarrow x+y \equiv_m x'+y']$

Sejam x, x', y, y' inteiros.

Suponha $x \equiv_m x'$ & $y \equiv_m y'$.

Como $x \equiv_m x'$, logo $x+y \equiv_m x'+y$ [$(+y)$ compatível] — por quê?

Como $y \equiv_m y'$, logo $x'+y \equiv_m x'+y'$ [$(+x')$ compatível] — por quê?

Logo $x+y \equiv_m x'+y'$.

∎

② $(\forall a, b, m)[a = b \Rightarrow a \equiv_m b]$ → $(\forall a, m)[a \equiv_m a]$

Sejam a, b, m inteiros tq $a = b$

Logo $a - b = 0$.

Como $m \mid 0$, logo $m \mid a-b$

Logo $a \equiv_m b$.

∎

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

Definição

a é inversível modulo m se, e somente se, existe um inteiro k tal que $ak = 1$ cadê o módulo?

① $(\forall a, m)[(a,m) = 1 \iff a$ é inversível modulo $m]$

Sejam a, m: int tq

$\Rightarrow$):

Suponha $(a,m) = 1$.

Sejam n, b: int tq $1 = an + mb$.

Calculemos:

$1 = an + mb$

$\equiv_m an + mb$

$\equiv_m an + 0b$

$\equiv_m an$

Escolha n.

$\Leftarrow$):

Suponha a inversível modulo m.

Seja a': int tq $aa' \equiv_m 1$, ou seja, $m \mid aa' - 1$.

Logo, k: int tq $aa' - 1 = mk$.

Logo, $1 = aa' - mk$

Basta demonstrar $(\exists t)[1 = ab + mt]$.

Escolho $a' = -k$

Logo $(a,m) = 1$.

por quê?

■

② $(\forall x, x', y, y', m)[x \equiv_m x' \wedge y \equiv_m y' \Rightarrow xy \equiv_m x'y']$

Sejam x, x', y, y', m inteiros

Suponha $x \equiv_m x' \wedge y \equiv_m y'$.

Como $x \equiv_m x'$, logo $xy \equiv_m x'y$ [(*) Comutável]

Como $y \equiv_m y'$, logo $x'y \equiv_m x'y'$ [(*) Comutável]

Logo $xy \equiv_m x'y'$.

■

③ $(\forall a, b, m)[a \equiv_m b \Rightarrow (\forall n)[a^n \equiv_m b^n]]$

Sejam a, b, m: int tq $a \equiv_m b$.

Indução em n.

Base: $a^0 \equiv_m b^0$.

Como $a^0 = 1$ e $b^0 = 1$, logo $a^0 = b^0$.

Logo $a^0 \equiv_m b^0$.

Passo indutivo $(\forall k)[a^k \equiv_m b^k \Rightarrow a^{k+1} \equiv_m b^{k+1}]$

Seja k: int tq $a^k \equiv_m b^k$.

Como $a \equiv_m b$ e $a^k \equiv_m b^k$, logo $aa^k \equiv_m bb^k$

Logo $a^{k+1} \equiv_m b^{k+1}$.

■

Só isso mesmo. RIP.

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

Def congruência (≡)

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

Congruência é compatível com

(+) $(\forall x)(\forall x')[x + x' \equiv_m x' + x]$ - isso é só a comutatividade de (+).

(·) Similar - Similar

(0) $(\forall x)[x \equiv_m 0]$ X

(1) Similar X

(-) Similar ? ⇒ ? $-a \equiv_m -b$

$a \equiv_m b \Rightarrow a + x \equiv_m b + x$ ✓

$a \equiv_m b \Rightarrow ax \equiv_m bx$ ✓

Lei do cancelamento somente quando a é coprimo com m!

$ca \equiv_m cb \Rightarrow a \equiv_m b$

Sejam $a, b, c, m > 0$ tq $(a, m) = 1$

Suponha $ca \equiv_m cb$

Cale $ca \equiv_m cb \Rightarrow c^{-1} \cdot ca \equiv_m c^{-1} cb$

$\Rightarrow a \equiv_m b$

isso sempre vale, tendo inversos.
O essencial aqui é como conseguir inversos.

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

Testamento (2/2)

PRO Congruência é compatível com a exponenciação (mesma base)

$a^n \equiv_m b^n \Rightarrow a \equiv_m b$, quando $(n, m) = 1$

- $\Theta\ (\forall a)[a^p \equiv_p a]$ com p primo
- $\Theta\ (\forall a)[a^{p-1} \equiv_p 1]$ com p primo & a, p coprimos
- $\Theta\ (p-1)! \equiv_p -1$, para qualquer p inteiro primo

Θ. Unicidade dos inversos mod m ~ o que significa?

Θ. $(a, m) = 1 \iff a$ tem inverso mod m

Θ. Teorema de Euler. $a^{\ell(m)} \equiv_m 1$ para todo a, m coprimos.

Demonstração. Esboço

Considere o conjunto $R = \{r_1, r_2, \dots, r_{\ell(m)}\}$ com todos r coprimos de $1 \leq r < m$. Agora considere o $aR = \{ar_1, ar_2, \dots, ar_{\ell(m)}\}$. Assim como $(a, m) = 1$ e $(r, m) = 1$, logo $(ar, m) = 1$, logo seus produtórios serão congruentes mod m, ou seja

↳ por quê?

$$ar_1 \cdot ar_2 \cdots ar_{\ell(m)} \equiv_m r_1 \cdot r_2 \cdots r_{\ell(m)}$$

Logo

$$a^{\ell(m)} \cdot r_1 \cdot r_2 \cdot r_3 \cdots r_{\ell(m)} \equiv_m r_1 \cdot r_2 \cdots r_{\ell(m)} \cdot 1$$

Logo

$$a^{\ell(m)} \equiv_m 1$$

Chegando na congruência desejada

DEF Função Totiente de Euler. Quantidade de coprimos com o m

$$\ell(m) \overset{\text{def}}{=} |\{i \in \{1, \dots, m\} \mid (i, m) = 1\}|$$

Θ p primo $\Rightarrow \ell(p) = p - 1$

Θ p primo $\Rightarrow \ell(p^k) = p^k - p^{(k-1)}$

$\Theta\ (X + Y)^p \equiv_p X^p + Y^p$

Demonstração p primo $\Rightarrow \ell(p) = p - 1$

Suponha p primo. Note que $1, \dots, p-1$ são coprimos com o p, pois $(p, p) = p \neq 1$. Logo temo $p-1$ coprimos com o p

o Sistema de resíduos completo (todos os coprimos) ~ não!

o Sistema de resíduos reduzido (de acordo com a congruência módulo um inteiro) ← o que significa isso?

Só isso mesmo. RIP.

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

Sejam a, b, m inteiros, dizemos que a e b são congruentes modulo m se m divide $a-b$. ✓

$$a \equiv_m b \stackrel{\text{def}}{=} m \mid a-b \quad ✓$$

A relação de congruência é compatível com $(\cdot)$ e $(+)$, mas não com a exponenciação, e isso é facilmente demonstrável com os teoremas que vocês tem envolvendo divisibilidade.

para algum ∃ / para todo ∀ / para onde / vírgula mágica

Chamamos também de sistema de resíduos completo um conjunto R_m se:

não há i nisso → inaceitável

$$R_m = \{\text{rem}(i,m) \mid (i,m)=1\}, \text{ para } i, m \text{ inteiros}$$

↳ Resto de i/m

$i \mid m$ é uma Prop''. → use comandos para estabelecer

Percebam que se $(a,m)=1$, então $aR_m \equiv_m R_m$. Vou demonstrar isso. ✓

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

Não. O s.r.c. generaliza os rem's que são obrigados a pertencer a um específico s.r.c.: o $\{0,1,\ldots,m-1\}$.

hw: Tem como demonstrar uma divisão de Euclides generalizada em qual o resto pertence a um fixo s.r.c. C?
$(\forall a)(\forall b \neq 0)(\forall C \text{ s.r.c.})(\exists! q,r)$
$[\, a = qb + r \;\&\; r \in C \,]$?

$aR_m \equiv R_m$

Testamento (2/2)

Sejam a, m: Int tq $(a,m) = 1$. e R um s.c.d.n. modulo m.
Ponto $aR \subseteq_m R$: --$\forall (x \in aR)\,[(\exists x')\,[x \equiv_m x' \wedge x \in R]$., com tempo :(

Seja $n \in R$. --Logo $an \in aR$.,
como $(a,m) = 1 = (n,m)$, logo $(an,m) = 1$.
Logo $(\exists x)\,[an \equiv_m x \wedge x \in R]$. -- R é um s.n.n, essa é uma propriedade.

Ponto $R \subseteq_m aR$:
Seja $n \in R$.
Logo $an \in aR$.
Xe...?

Considere:
$\varphi(n) = |Rn|$
↳ s.n.n modulo n

Assim não fica bem definida a φ.
(Por quê?)

Seja m: Int t.q m é primo, temos como teorema que se $(a,m) = 1$, então $a^{\varphi(m)} \equiv_m 1$. Vou demonstrar isso.

Com m é primo, logo $\varphi(m) = m - 1$.
Seja $R = \{n_1, n_2, n_3, \ldots, n_{m-1}\}$ um s.n.n modulo m.
Logo $aR \equiv_m R$, e logo $an_1 \cdot an_2 \ldots aR_{m-1} \equiv n_1 \cdot n_2 \ldots n_{m-1}$.
Logo $a^{m-1}\left(\prod_{i=1}^{m-1} n_i\right) \equiv_m \left(\prod_{i=1}^{m-1} n_i\right)$, e logo $a^{m-1} \equiv_m 1$.
Logo $a^{\varphi(m)} \equiv_m 1$.
-- há um teorema que diz que isso é, produto é congruente modulo m com 1.

o ponto disso é que vale para não-primos também.

nem foi tanto, pois tu assumiu m primo antes.

Prove que ganhamos gratuitamente que para qualquer primo p se $(a,p) = 1$, então $a^{p-1} \equiv_p 1$ e, por consequência, $a^p \equiv_p a$.

Outros Teoremas: -- (considere p sempre um primo)
$(\forall a,b,p)\,[(a+b)^p \equiv_p a^p + b^p]$
$(\forall a,b,n,m)\,[(n,m) = 1 \wedge an \equiv_m bn \Rightarrow a \equiv_m b]$

melhor estabelecer inversos do que cancelamento pois

inv $\Rightarrow$ can
mas
can $\not\Rightarrow$ inv.

Só isso mesmo. RIP.

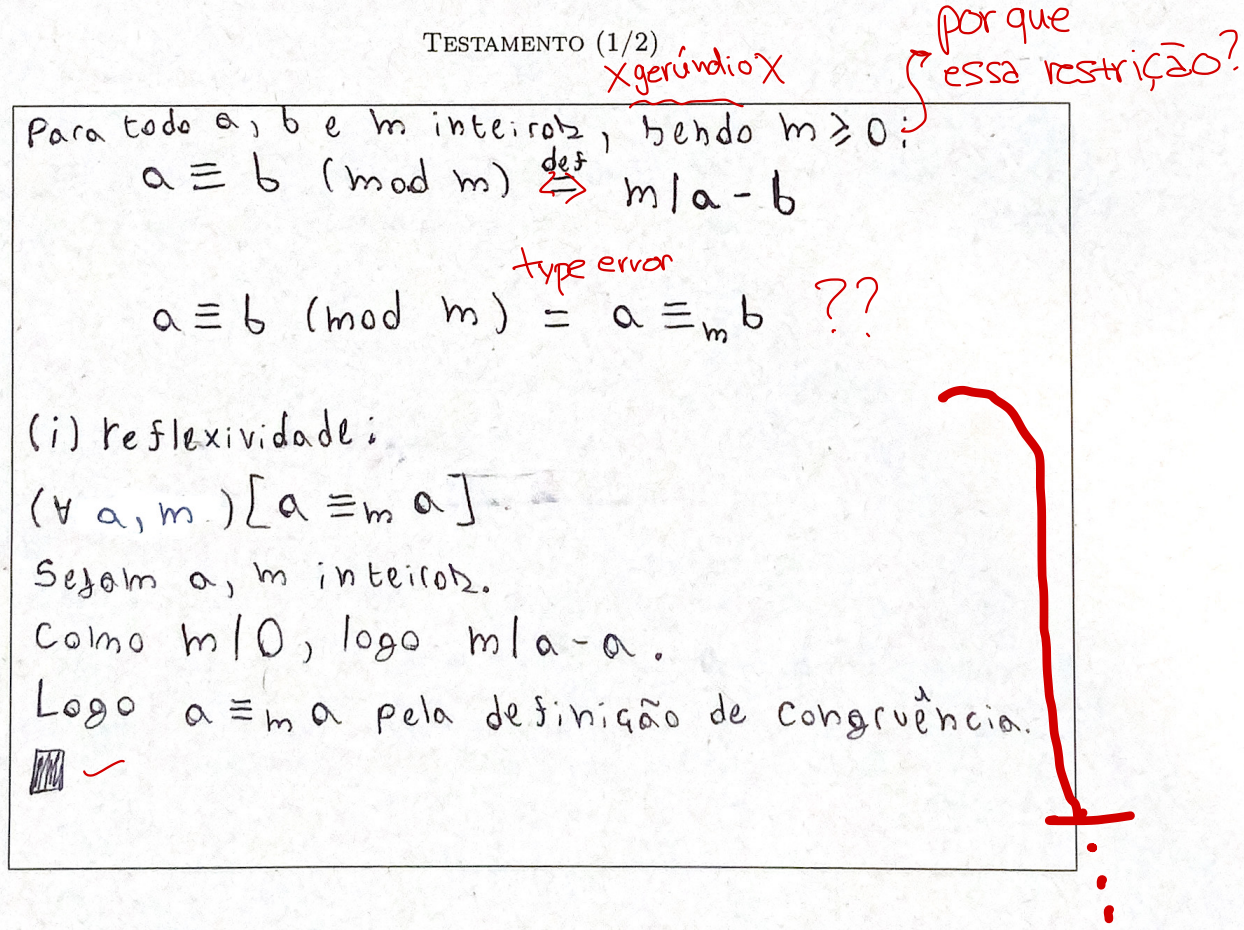
(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)



[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

Foi literalmente o exemplo que dei sobre o que não escolher para demonstrar

TESTAMENTO (2/2)

(ii) Transitividade:

$(\forall a,b,c,m)[a \equiv_m b \ \& \ b \equiv_m c \Rightarrow a \equiv_m c]$

Sejam a,b,c,m inteiros tal que $a \equiv_m b \ \& \ b \equiv_m c$.

Como $a \equiv_m b \ \& \ b \equiv_m c$, logo $m \mid a-b \ \& \ m \mid b-c$.

logo $m \mid (a-b)+(b-c)$.

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

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

$= a+(0-c)$

$= a-c$

Como $m \mid a-c$, logo $a \equiv_m c$.

(iii) Simetria:

$(\forall a,b,m)[a \equiv_m b \Leftrightarrow b \equiv_m a]$

Seja a,b,m inteiros.

($\Rightarrow$): Suponha $a \equiv_m b$, ou seja $m \mid a-b$, logo $m \mid (a-b)(-1)$

Logo $m \mid (b-a)$, ou seja $b \equiv_m a$.

($\Leftarrow$): Similar.

Propriedades: Sejam a,b,c e m inteiros:

(i): $-a \equiv_m -b$ (ii): $ac \equiv_m bc$ (iii): $a+c \equiv_m b+c$

X X X

Só isso mesmo. RIP.

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

~~Definição congruência~~

Def. (congruência) Sejam $a, b, m : \text{Int}$ tq $m > 0$ (por quê??)

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

Podemos mostrar a equivalência entre essa definição e a intuição de que os restos da divisão de Eutlides são iguais. (ah, foi por isso?)

ESBOÇO: Para a ($\Rightarrow$) basta mostrar como usar o Lema de Bezout pode concluir que $r_a = r_b$. Na ($\Leftarrow$), trabalhando com $r_a - r_b$ chegamos a $m \mid a-b$. Não dá para entender. Parece que uma demonstração teria sido mais curta que esse "esboço".

Θ. A congruência é uma relação de equivalência.

ESBOÇO: Usando apenas a definição podemos mostrar todas as reflexividade, transitividade e simetria.

A partir disso podemos "dividir" o $\mathbb{Z}$ em classes de equivalência ~~para algum inteiro m~~. módulo m, para $m \in \mathbb{Z}_{>0}$. (sem essa restrição!!)

Propriedades A congruência possui os seguinte, para $a \equiv b \pmod m$

(I) $a + c \equiv b + c \pmod m$

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

Como esse esboço ajuda?

(Existe teorema cuja demonstração não "se baseia" nas definições?)

TESTAMENTO (2/2)

$ac \equiv bc \pmod m$

$-a \equiv -b \pmod m$

ESBOÇO: A demonstração se baseia na definição.

Def. (inverso mod m) Sejam $a, m > 0$: Int. Um inverso mod m de a é definido como

$a a' \equiv 1 \pmod m$? → não faz sentido

Para determinar a notação $(^{-1})$ deveremos demonstrar o seguinte.

Θ. (unicidade do inverso mod m).

ESBOÇO: Com os inversos b, b' de a mod m e pela transitividade obtemos $ab \equiv ab' \pmod m$. A partir de algumas propriedades concluímos a demonstração. } muito handwaving

Θ. Quando $a = b$ temos também $a \equiv b \pmod m$, para algum $m > 0$. Algum? Qual??

ESBOÇO: Reflexividade da ~~cong~~ $(\equiv)$ e ~~da $(=)$~~.

A existência dos inversos é garantida sob as seguinte condições

Θ. a tem inverso mod m $\Leftrightarrow (a, m) = 1$ ✓

ESBOÇO: $(\Rightarrow)$

$(\Leftarrow)$ usando Lema de Bezout e outras propriedades. } Vago demais

Isso nos garante que

Θ. Para $m > 0$, quando m é primo todos terão inverso.

ESBOÇO: consequência direta do teorema anterior

Só isso mesmo. RIP.

(64) **C**

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

Definições & teoremas precisam de texto & contexto!

TESTAMENTO (1/2)

A, B, m : ?

$A \equiv_m B \overset{\text{def}}{\iff} m \mid A - B \overset{\text{def}}{\iff} A \equiv B \pmod m$

X

$\equiv_m$ Respeita a estrutura algébrica dos Int ✓ ...mas o que isso significa?

(Ex.:)

$\Theta.\ (\forall a, b, c, \in_m \text{Int})\ [\, a + c \equiv_m b + c \Rightarrow a \equiv_m b \,]$:

sejam $a, b, c, m \in \text{Int}$ t.q. $a + c \equiv_m b + c$, ou seja $m \mid (a+c)-(b+c)$

Calculemos:

$$\begin{aligned}(a+c)-(b-c) &= a + c - b - c \\ &= a - b + (c - c) \\ &= a - b\end{aligned}$$

Logo $m \mid a - b$, ou seja $a \equiv_m b$.

(Os demais são semelhantes) ?

Ⓐ

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

Θ. $(\forall a, b : Int)\ [\ a \equiv_0 b \Rightarrow a = b\ ]$ ✓

sejam $a, b : Int$ T.q. $a \equiv_0 b$ ou seja $0 \mid a - b$
Como 0 só divide 0, logo $a - b = 0$
logo $a = b$.

não faz sentido esse uso de aspas.

Θ. $(\forall m, n : Int)\ [\ n \equiv_m 0 \Rightarrow m \mid n\ ]$ ✓

seja $m, n : Int$ T.q. $n \equiv_m 0$, ou seja $m \mid 0 - n$
Logo $m \mid -n$
Como $-n$ é oposto de n, logo $m \mid n$

Θ. $(\forall, m, n, p : \mathbb{N})\ [\ p \text{ é Primo} \Rightarrow m^{\varphi(n)} \equiv_p 1\ ]$ nem esboço?

Θ. $(\forall a : Int)\ [\ a \equiv_m a\ ]$:

seja $m, a : Int$ ~~T.q. $a \equiv_m a$, queremos mostrar a~~

~~Logo~~
Calculemos:

$$\begin{aligned} a \equiv_m a &= m \mid a - a \\ &= m \mid 0 \end{aligned}$$

Imediato.

~~Θ. (∀~~
a é Par $\overset{\text{def (num)}}{\Leftrightarrow}$ $a \equiv_2 0$

Θ. Sistema Posicional (Usar ~~modulo~~ "$\equiv_m$" para tratar bases numéricas) ??

Θ. $(\forall a, b, c, m : Int)\ [\ a \equiv_m b\ \&\ b \equiv_m c \Rightarrow a \equiv_m c\ ]$

Θ. (Existe uma forma de testar Primos!)
??

??

(Existem mais Exigências que não Posso demonstrar / Continuem o Trabalho) (e não falhem)

Só isso mesmo. RIP.

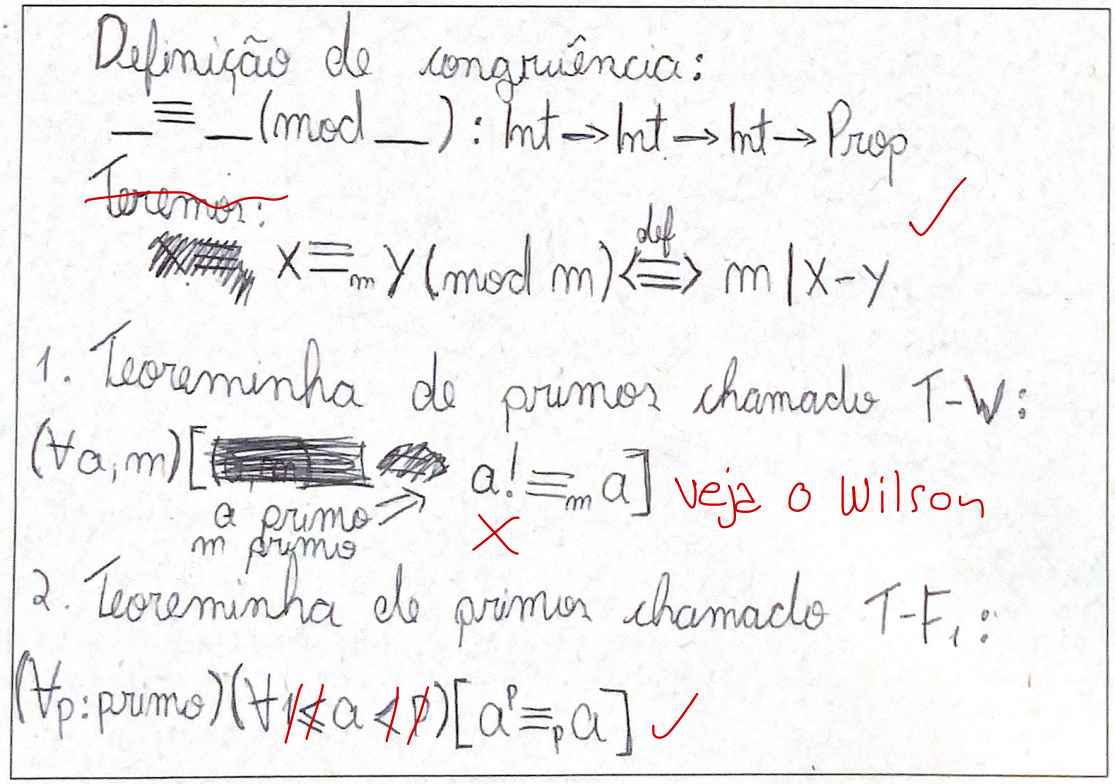
(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)



[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

3- Teoreminha chamado T-F_2:
$(\forall p: \text{primo})(\forall 1 \leq a < p)[a^{(p-1)} \equiv_p 1]$

Esboço de T-F_1:
Considere o T-F_2 como demonstrado.
Logo $a \cdot a^{(p-1)} \equiv_p a \cdot 1$
Logo $a^p \equiv_p a$. ∎

~~Definição de inversível~~
~~a é inversível mod m sse~~
$(a, m) = 1$ ~~sse~~

Teorema de inverso mod m:
a tem inverso mod m sse $(a, m) = 1$.

~~Sistema~~ Definição de sistema de resíduos completo em m.
Conjunto de tamanho m em que cada
o que é isso? ← tinha tem um único ~~representante~~ mod m. ??

Definição de sistema de resíduos reduzidos mod m:
Seja C um sistema de resíduos completo mod m.
$s.r.r. \overset{def}{\Longleftrightarrow} \{x \in C \mid (x, m) = 1\}$ ← (muito) type error

Definição de $\varphi(m)$:
$\varphi(m) \overset{def}{=} \{x \in \{y \mid 1 \leq y \leq m\} \mid (x, m) = 1\}$

4- Teorema da φ ser multiplicativa:
$(\forall m, n)[(m, n) = 1 \Rightarrow \varphi(mn) = \varphi(m) \cdot \varphi(n)]$

Esboço da φ multiplicativa: Considere a matriz $m \times n$.
Caso um elemento de qualquer coluna seja coprimo com m, a coluna inteira será também.
Qualquer coluna de $m \times n$ é um s.r.c de m e tem um s.r.r de m ??

Só isso mesmo. RIP.

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

nada disso faz sentido

TESTAMENTO (1/2)

$\overset{\text{def}}{=\!=}$ dois Var de mesmo Type são iguais ($=$) ou seus resultados de soma ($+$), multiplicação ($\cdot$), divisão ($\_/\_$), entre outros, são congruentes entre si; os dois Var iniciais, também, são congruentes ($\equiv$) entre si.

~~$a \overset{\text{def}}{=\!=} b$~~

$a \equiv b \overset{\text{def}}{=\!=} ax(=\vee\equiv)bx$ e $a/x(=\vee\equiv)bx$

~~$a \overset{\text{def}}{=\!=}_x b$~~

$a \equiv_x b$ ou $a \equiv b \pmod{x} \overset{\text{def}}{=\!=} a/x = q_2 + r_1$ e $b/x = q_2 + r_2$

~~fonte~~ (qualquer divisão ($\_/\_$)) gera quociente e resto, representados

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

por q_1 e q_2 e Λ_1 e Λ_2).

onde $\Lambda_1 = \Lambda_2$.

Θ. $(\forall x, y : \text{Int})[y \equiv x$, onde $xy \equiv x/y$, $x \equiv y \equiv 1]$.

ou $ba \equiv b/a \overset{\text{def}}{\equiv} b \equiv a$ $[b = a = 1]$.

$c/d \equiv e/f$ se $c \equiv e$ e $d \equiv f$.

$\frac{a}{b} \equiv \frac{b}{a} \overset{\text{def}}{\equiv} a \equiv b$, logo $b \equiv a$.

Θ.

$a/b = q_1 + \Lambda_1 \; c/b = q_2 + \Lambda_2$, onde: $q_1 \equiv q_2$ e $\Lambda_1 \equiv \Lambda_2$, se somente se, $a \equiv c$.

Só isso mesmo. RIP.

(64) C

Sentindo uma picadinha no pé tu acabou de acordar dum sono profundo e descubriu que tudo que tens estudado *sobre congruências e aritmética modular* fez parte dum sonho—junto com o mundo em qual tal estudos aconteceram. Acordando, tu lembra que: o povo no teu mundo real conhece os inteiros, suas operações, e todas suas propriedades que estudamos pré-congruências, e até usa a mesma notação e nomenclatura. Mas ninguém nesse mundo pensou em definir a relação de congruência módulo um inteiro e logo nada que surgiu a partir dela no teu sonho é conhecido!

Infelizmente a picadinha no pé que te acordou foi duma cobra letal e *em exatamente 48' tu vai morrer*. Por algum motivo *tua única preocupação* é compartilhar com o mundo as coisas mais legais que descobriu nesse sonho maluco.[3] A única coisa que tu tens na tua frente é pouco papel e umas canetas. É óbvio que *não tem como escrever tudo que sonhou*—tanto por motivos de espaço, quanto por motivos de cobra. Tu vai ter de deixar uns teoremas sem demonstração (ou com apenas esboço de demonstração) e pular uns assuntos completamente. *Essas escolhas são tua responsabilidade (e logo escolher bem faz parte desta avaliação).*

Bom testamento!

TESTAMENTO (1/2)

• Definição: Sejam a, b, m inteiros
Dizemos que a é congruente com b módulo m sse m divide $a-b$. Em símbolos: $a \equiv_m b \overset{def}{\Leftrightarrow} m \mid a-b$

• Teoremas:

θ_1. $\equiv_m$ é uma relação de equivalência ✓

θ_2. $\equiv_m$ é compatível com as operações dos inteiros, ✓

ou seja: ✓

$$(\forall c, c')\left[c \equiv_m c' \Rightarrow \begin{cases} (\forall a)\,[c+a \equiv_m c'+a] & \text{①} \\ (\forall a)\,[c \cdot a \equiv_m c' \cdot a] & \text{②} \\ -c \equiv_m -c' & \text{③} \end{cases} \right]$$

① $(+a)$ – compat
② $(\cdot a)$ – compat

• Esboço da demonstração de θ_2:
Sejam R t.q. $m \cdot R = c - c'$
Parte 1: Escolho R como testemunha
Parte 2: Escolho $a \cdot R$ como testemunha
Parte 3: Escolho $-R$ como testemunha

não precisa "baixar" o nível até abrir a definição da (1).
Como $m \mid c - c'$, logo $m \mid (c+a) - (c'+a)$

[3] Sim, tu já pulou os Cinco Estágios do Luto e foi diretamente para o sexto: *escrever matemática linda sem estresse.*

(low-level demais!)

TESTAMENTO (2/2)

θ_3: $(\forall a, m)\,[(a,m)=1 \Leftrightarrow (\exists a')[aa' \equiv_m 1]]$

Demonstração θ_3:

Parte $\Rightarrow$:

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

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

Calculamos: $1 = ax + my$ $[\theta_4]$

$\equiv_m ax + 0y$ $[\theta_3]$

$\equiv_m ax + 0$

$\equiv_m ax$

Escolho x como testemunha

imediato

Parte $\Leftarrow$:

Sejam a, m inteiros t.q. $(\exists a')[aa' \equiv_m 1]$

Seja a' t.q. $aa' \equiv_m 1$

Seja k t.q. $m \cdot k = aa' - 1$

aproveite o Lema de Bézout!

Parte ida:

imediato.

Parte $1 \mid m$:

imediato

Parte $(\forall m')[m' \mid a \wedge m' \mid m \Rightarrow m' \mid 1]$

Sejam m' t.q. $m' \mid a \wedge m' \mid m$

Logo, seja $k_{a'}$ t.q. $m' \cdot k_{a'} = a$

Seja $k_{m'}$ t.q. $m' \cdot k_{m'} = m$

Escolho $k_{m'} \cdot k$ como testemunha

Calculamos:

$m' \cdot (k_{a'} a' - k_{m'} \cdot k) = m' k_{a'} a' - m' k_{m'} \cdot k$

$= aa' - m \cdot k$

$= aa' - (aa' - 1)$

$= aa' - aa' + 1$

$= 1$

θ_4: $(\forall m)\,[m \equiv_m 0]$

Esboço: $(\forall m)[m \mid m]$

θ_5: $(\forall a, p)\,[p \text{ primo} \Rightarrow a^p \equiv_p a]$

~~θ_6: $(\forall b, b', m, m')[(\exists x)[x \equiv_m b \wedge x \equiv_{m'} b']$~~

~~Esboço da demonstração do θ_6~~

~~Sejam b, b', m, m' inteiros,~~

~~Escolho~~ não é único!!

θ_6: $(\forall b_1, b_2, m_1, m_2)\,[m_1, m_2 \text{ coprimos} \Rightarrow (\exists! x)[x \equiv_{m_1} b_1 \wedge x \equiv_{m_2} b_2]]$

Esboço da demonstração do θ_6:

Sejam b_1, b_2, m_1, m_2 inteiros, t.q. $(m_1, m_2) = 1$

Logo, $(\exists m_1')[m_1 m_1' \equiv_{m_2} 1]$, pelo θ_3.

Logo, seja m_1' t.q. $m_1 m_1' \equiv_{m_2} 1$ ✓

Escolho $m_1' \cdot m_1 \cdot (b_2 - b_1) + b_1$ como testemunha.

✓

Só isso mesmo. RIP.