Algoritmos y Estructuras de Datos I

Practico 3

(Algoritmo de la división)

Damián Barsotti

Fa.M.A.F., Universidad Nacional de Córdoba, Argentina

Algoritmo de la división

Problema

Dados dos números, hay que encontrar el cociente y el resto de la división entera entre ellos.

Algoritmo de la división

Problema

Dados dos números, hay que encontrar el cociente y el resto de la división entera entre ellos.

Especificación

Var $x, y, q, r : Int$;
$\{P : x \geq 0 \wedge y > 0\}$
S
$\{Q : x = q * y + r \wedge 0 \leq r \wedge r < y\}$
Donde x, y no cambian.

Algoritmo de la división

Problema

Dados dos números, hay que encontrar el cociente y el resto de la división entera entre ellos.

Especificación

Var $x, y, q, r : Int$;
$\{P : x \geq 0 \wedge y > 0\}$
S
$\{Q : x = q * y + r \wedge 0 \leq r \wedge r < y\}$
Donde x, y no cambian.

Resultado como relacion entre variables.

Pasos para derivar una repetición

Ver doc "Pasos Sugeridos para Derivar una Repetición"

1. Encontrar invariante candidato.

Pasos para derivar una repetición

Ver doc “Pasos Sugeridos para Derivar una Repetición”

1. Encontrar invariante candidato.
2. Inicialización.

Pasos para derivar una repetición

Ver doc "Pasos Sugeridos para Derivar una Repetición"

1. Encontrar invariante candidato.
2. Inicialización.
3. Finalización.

Pasos para derivar una repetición

Ver doc "Pasos Sugeridos para Derivar una Repetición"

1. Encontrar invariante candidato.
2. Inicialización.
3. Finalización.
4. Encontrar cota candidata.

Pasos para derivar una repetición

Ver doc “Pasos Sugeridos para Derivar una Repetición”

1. Encontrar invariante candidato.
2. Inicialización.
3. Finalización.
4. Encontrar cota candidata.
5. Cuerpo del bucle.

Pasos para derivar una repetición

Ver doc “Pasos Sugeridos para Derivar una Repetición”

1. Encontrar invariante candidato.
2. Inicialización.
3. Finalización.
4. Encontrar cota candidata.
5. Cuerpo del bucle.
6. Cota positiva.

Pasos para derivar una repetición

Ver doc "Pasos Sugeridos para Derivar una Repetición"

1. Encontrar invariante candidato.
2. Inicialización.
3. Finalización.
4. Encontrar cota candidata.
5. Cuerpo del bucle.
6. Cota positiva.
7. Cota disminuye.

Técnica para encontrar invariante candidato

Tomar términos de una conjunción

Técnica para encontrar invariante candidato

Tomar términos de una conjunción

- Por paso 3 (finalizacion)

$$I \land \neg B \Rightarrow Q$$

Técnica para encontrar invariante candidato

Tomar términos de una conjunción

- Por paso 3 (finalizacion)

$$I \land \neg B \Rightarrow Q$$

- Hagamos $I \land \neg B = Q$

Técnica para encontrar invariante candidato

Tomar términos de una conjunción

- Por paso 3 (finalizacion)

$$I \wedge \neg B \Rightarrow Q$$

- Hagamos $I \wedge \neg B \;=\; Q$
- Por lo tanto

Técnica para encontrar invariante candidato

Tomar términos de una conjunción

- Por paso 3 (finalizacion)

$$I \wedge \neg B \Rightarrow Q$$

- Hagamos $I \wedge \neg B = Q$
- Por lo tanto
  1. En Q tiene haber conjunciones

Técnica para encontrar invariante candidato

Tomar términos de una conjunción

- Por paso 3 (finalizacion)

$$I \wedge \neg B \Rightarrow Q$$

- Hagamos $I \wedge \neg B = Q$
- Por lo tanto
  1. En Q tiene haber conjunciones
  2. Algunos términos son I y otros son $\neg B$

Técnica para encontrar invariante candidato

Tomar términos de una conjunción

- Por paso 3 (finalizacion)

$$I \wedge \neg B \Rightarrow Q$$

- Hagamos $I \wedge \neg B \; = \; Q$
- Por lo tanto
  1. En Q tiene haber conjunciones
  2. Algunos términos son I y otros son $\neg B$
- En algoritmo de la división:

$$Q : x = q * y + r \wedge 0 \leq r \wedge r < y$$

1. Invariante candidato y guarda

$$Q : x = q * y + r \wedge 0 \leq r \wedge r < y$$

- $x = q * y + r$ contiene las variables resultado

1. Invariante candidato y guarda

$$Q : x = q * y + r \land 0 \leq r \land r < y$$

- $x = q * y + r$ contiene las variables resultado

$\Rightarrow$ debería ser invariante.

1. Invariante candidato y guarda

$$Q : x = q * y + r \wedge 0 \leq r \wedge r < y$$

- $x = q * y + r$ contiene las variables resultado

$\Rightarrow$ debería ser invariante.

- Al final r dentro del intervalo $[0, y)$

1. Invariante candidato y guarda

$$Q : x = q * y + r \wedge 0 \leq r \wedge r < y$$

- $x = q * y + r$ contiene las variables resultado

$\Rightarrow$ debería ser invariante.

- Al final r dentro del intervalo $[0, y)$

$\Rightarrow$ dentro del bucle no debería ser $r < 0$

$\ldots$
do $r < 0 \rightarrow$
    $\ldots$
od

1. Invariante candidato y guarda

$$Q : x = q * y + r \wedge 0 \leq r \wedge r < y$$

- $x = q * y + r$ contiene las variables resultado

$\Rightarrow$ debería ser invariante.

- Al final r dentro del intervalo $[0, y)$

$\Rightarrow$ dentro del bucle no debería ser $r < 0$

...
do $r < 0 \rightarrow$
    ...
od

$\Rightarrow$ $0 \leq r$ debería ser invariante.

1. Invariante candidato y guarda

$$Q : x = q * y + r \wedge 0 \leq r \wedge r < y$$

- $x = q * y + r$ contiene las variables resultado

$\Rightarrow$ debería ser invariante.

- Al final r dentro del intervalo $[0, y)$

$\Rightarrow$ dentro del bucle **no** debería ser $r < 0$

```
...
do r < 0 →
    ...
od
```

$\Rightarrow$ $0 \leq r$ debería ser invariante.

- Por descarte, $r < y$ debería ser $\neg B$

1. Invariante candidato y guarda

$$Q : x = q * y + r \wedge 0 \leq r \wedge r < y$$

- $x = q * y + r$ contiene las variables resultado

$\Rightarrow$ debería ser invariante.

- Al final r dentro del intervalo $[0, y)$

$\Rightarrow$ dentro del bucle no debería ser $r < 0$

...
do $r < 0 \rightarrow$
    ...
od

$\Rightarrow$ $0 \leq r$ debería ser invariante.

- Por descarte, $r < y$ debería ser $\neg B$

$$I : x = q * y + r \wedge 0 \leq r \qquad B : r \geq y$$

2. Inicialización

No se cumple

$P : x \geq 0 \wedge y > 0 \Rightarrow I : x = q * y + r \wedge 0 \leq r$

2. Inicialización

No se cumple

$P : x \geq 0 \wedge y > 0 \Rightarrow I : x = q * y + r \wedge 0 \leq r$

Agrego inicialización:

2. Inicialización

No se cumple

$P : x \geq 0 \wedge y > 0 \Rightarrow I : x = q * y + r \wedge 0 \leq r$

Agrego inicialización:

- Despejar **E** y **F** de

$$\{P\}$$
$$q, r := \mathbf{E}, \mathbf{F}$$
$$\{I\}$$

2. Inicialización

No se cumple

$P : x \geq 0 \wedge y > 0 \;\Rightarrow\; I : x = q * y + r \wedge 0 \leq r$

Agrego inicialización:

- Despejar **E** y **F** de

$$\begin{array}{c} \{P\} \\ q, r := \mathbf{E}, \mathbf{F} \\ \{I\} \end{array}$$

$=$ Encontrar **E** y **F** tal que

$$P \Rightarrow wp.(q, r := \mathbf{E}, \mathbf{F}).I$$

sea verdadera.

2. Inicialización

No se cumple

$P : x \geq 0 \wedge y > 0 \;\Rightarrow\; I : x = q * y + r \wedge 0 \leq r$

Agrego inicialización:

- Despejar **E** y **F** de

$$\begin{array}{c} \{P\} \\ q, r := \mathbf{E}, \mathbf{F} \\ \{I\} \end{array}$$

$=$ Encontrar **E** y **F** tal que

$$P \Rightarrow wp.(q, r := \mathbf{E}, \mathbf{F}).I$$

sea verdadera.

$=$ Suponer P y encontrar **E** y **F** tal que

$$wp.(q, r := \mathbf{E}, \mathbf{F}).I$$

sea verdadera.

2. Inicialización

Programa anotado a derivar

Var $x, y, q, r : Int$;
$\{P : x \geq 0 \wedge y > 0\}$
$q, r := \mathbf{E}, \mathbf{F}$; ?
$\{I : x = q * y + r \wedge 0 \leq r\}$
do $r \geq y \rightarrow$
S ?
od
$\{I \wedge \neg B : x = q * y + r \wedge 0 \leq r \wedge r < y\}$?
$\{Q : x = q * y + r \wedge 0 \leq r \wedge r < y\}$

2. Inicialización

Derivación

2. Inicialización

Derivación

Sup $P : x \geq 0 \land y > 0$

$wp.(q, r := \mathbf{E}, \mathbf{F}).(x = q * y + r \land 0 \leq r)$

2. Inicialización

Derivación

Sup $P : x \geq 0 \ \wedge \ y > 0$

$$
\begin{array}{ll}
 & wp.(q, r := \mathbf{E}, \mathbf{F}).(x = q * y + r \ \wedge \ 0 \leq r) \\
\equiv & \{ \text{ Def } wp \ \} \\
 & x = \mathbf{E} * y + \mathbf{F} \ \wedge \ 0 \leq \mathbf{F}
\end{array}
$$

2. Inicialización

Derivación

Sup $P : x \geq 0 \wedge y > 0$

$$
\begin{aligned}
& wp.(q, r := \mathbf{E}, \mathbf{F}).(x = q * y + r \wedge 0 \leq r) \\
\equiv\ & \{ \text{ Def } wp \text{ } \} \\
& x = \mathbf{E} * y + \mathbf{F} \wedge 0 \leq \mathbf{F} \\
\equiv\ & \{ \text{ Hacemos } \mathbf{F} \leftarrow x \text{ } \} \\
& x = \mathbf{E} * y + x \wedge 0 \leq x
\end{aligned}
$$

2. Inicialización

Derivación

Sup $P : x \geq 0 \wedge y > 0$

$$
\begin{array}{ll}
 & wp.(q, r := \mathbf{E}, \mathbf{F}).(x = q * y + r \wedge 0 \leq r) \\
\equiv & \{ \text{ Def } wp \ \} \\
 & x = \mathbf{E} * y + \mathbf{F} \wedge 0 \leq \mathbf{F} \\
\equiv & \{ \text{ Hacemos } \mathbf{F} \leftarrow x \ \} \\
 & x = \mathbf{E} * y + x \wedge 0 \leq x \\
\equiv & \{ \text{ Sup } x \geq 0 \ \} \\
 & x = \mathbf{E} * y + x
\end{array}
$$

2. Inicialización

Derivación

Sup $P : x \geq 0 \wedge y > 0$

$$
\begin{aligned}
& wp.(q, r := \mathbf{E}, \mathbf{F}).(x = q * y + r \wedge 0 \leq r) \\
\equiv \; & \{ \text{ Def } wp \text{ } \} \\
& x = \mathbf{E} * y + \mathbf{F} \wedge 0 \leq \mathbf{F} \\
\equiv \; & \{ \text{ Hacemos } \mathbf{F} \leftarrow x \text{ } \} \\
& x = \mathbf{E} * y + x \wedge 0 \leq x \\
\equiv \; & \{ \text{ Sup } x \geq 0 \text{ } \} \\
& x = \mathbf{E} * y + x \\
\equiv \; & \{ \text{ Aritmética } \} \\
& 0 = \mathbf{E} * y
\end{aligned}
$$

2. Inicialización

Derivación

Sup $P : x \geq 0 \land y > 0$

$$
\begin{aligned}
& wp.(q, r := \mathbf{E}, \mathbf{F}).(x = q * y + r \land 0 \leq r) \\
\equiv & \ \{ \text{ Def } wp \ \} \\
& x = \mathbf{E} * y + \mathbf{F} \land 0 \leq \mathbf{F} \\
\equiv & \ \{ \text{ Hacemos } \mathbf{F} \leftarrow x \ \} \\
& x = \mathbf{E} * y + x \land 0 \leq x \\
\equiv & \ \{ \text{ Sup } x \geq 0 \ \} \\
& x = \mathbf{E} * y + x \\
\equiv & \ \{ \text{ Aritmética } \} \\
& 0 = \mathbf{E} * y \\
\equiv & \ \{ \text{ Aritmética y sup. } y > 0 \ \} \\
& 0 = \mathbf{E}
\end{aligned}
$$

2. Inicialización

Derivación

Sup $P : x \geq 0 \wedge y > 0$

$$
\begin{array}{ll}
& wp.(q, r := \mathbf{E}, \mathbf{F}).(x = q * y + r \wedge 0 \leq r) \\
\equiv & \{ \text{ Def } wp \text{ } \} \\
& x = \mathbf{E} * y + \mathbf{F} \wedge 0 \leq \mathbf{F} \\
\equiv & \{ \text{ Hacemos } \mathbf{F} \leftarrow x \text{ } \} \\
& x = \mathbf{E} * y + x \wedge 0 \leq x \\
\equiv & \{ \text{ Sup } x \geq 0 \text{ } \} \\
& x = \mathbf{E} * y + x \\
\equiv & \{ \text{ Aritmética } \} \\
& 0 = \mathbf{E} * y \\
\equiv & \{ \text{ Aritmética y sup. } y > 0 \text{ } \} \\
& 0 = \mathbf{E} \\
\equiv & \{ \text{ Hacemos } \mathbf{E} \leftarrow 0 \text{ } \} \\
& \mathit{True}
\end{array}
$$

2. Inicialización

El programa queda por ahora

Var $x, y, q, r : Int$;
$\{P : x \geq 0 \wedge y > 0\}$
$q, r := 0, x$; ♡
$\{I : x = q * y + r \wedge 0 \leq r\}$
do $r \geq y \rightarrow$
S ?
od
$\{I \wedge \neg B : x = q * y + r \wedge 0 \leq r \wedge r < y\}$?
$\{Q : x = q * y + r \wedge 0 \leq r \wedge r < y\}$

3. Finalización

Hay que demostrar

$$I \wedge \neg B \Rightarrow Q$$

3. Finalización

Hay que demostrar

$$I \wedge \neg B \Rightarrow Q$$

Var $x, y, q, r : Int$;
$\{P : x \geq 0 \wedge y > 0\}$
$q, r := 0, x$; ♡
$\{I : x = q * y + r \wedge 0 \leq r\}$
do $r \geq y \rightarrow$
S ?
od
$\{I \wedge \neg B : x = q * y + r \wedge 0 \leq r \wedge r < y\}$?
$\{Q : x = q * y + r \wedge 0 \leq r \wedge r < y\}$

3. Finalización

Esta demostrado

ya que por técnica $I \wedge \neg B = Q$.

3. Finalización

Esta demostrado

ya que por técnica $I \wedge \neg B = Q$.

Var $x, y, q, r : Int$;
$\{P : x \geq 0 \wedge y > 0\}$
$q, r := 0, x$; ♡
$\{I : x = q * y + r \wedge 0 \leq r\}$
do $r \geq y \rightarrow$
S ?
od
$\{I \wedge \neg B : x = q * y + r \wedge 0 \leq r \wedge r < y\}$ ♡
$\{Q : x = q * y + r \wedge 0 \leq r \wedge r < y\}$

4. Encontrar cota candidata t

- Se tiene que cumplir

$$I \wedge B : x = q * y + r \wedge 0 \leq r \wedge B \Rightarrow t \geq 0$$

4. Encontrar cota candidata t

- Se tiene que cumplir

$$I \wedge B : x = q * y + r \wedge 0 \leq r \wedge B \Rightarrow t \geq 0$$

- En I $r \geq 0$

4. Encontrar cota candidata t

- Se tiene que cumplir

$$I \wedge B : x = q * y + r \wedge 0 \leq r \wedge B \Rightarrow t \geq 0$$

- En I $r \geq 0$
- Para terminar se debe falsificar $B : r \geq y$ (cota disminuye)

do $r \geq y \rightarrow$
S
od

4. Encontrar cota candidata t

- Se tiene que cumplir

$$I \wedge B : x = q * y + r \wedge 0 \leq r \wedge B \Rightarrow t \geq 0$$

- En I $r \geq 0$
- Para terminar se debe falsificar $B : r \geq y$ (cota disminuye)

  do $r \geq y \rightarrow$
  S
  od
- Probemos $t : r$

5. Cuerpo del bucle

Pruebo con asignación

5. Cuerpo del bucle

Pruebo con asignación

- r debe disminuir (es la cota).

5. Cuerpo del bucle

Pruebo con asignación

- r debe disminuir (es la cota).
- Despejar **E** y **k** de

$$\{I \ \wedge \ B\}$$
$$q, r := \mathbf{E}, r - \mathbf{k}$$
$$\{I\}$$

con $\mathbf{k} > 0$.

5. Cuerpo del bucle

Pruebo con asignación

- r debe disminuir (es la cota).
- Despejar **E** y **k** de

$$\begin{gathered}\{I \wedge B\}\\ q, r := \mathbf{E}, r - \mathbf{k}\\ \{I\}\end{gathered}$$

con $\mathbf{k} > 0$.

$=$ Encontrar **E** y **k** tal que

$$I \wedge B \Rightarrow wp.(q, r := \mathbf{E}, r - \mathbf{k}).I$$

sea verdadera.

5. Cuerpo del bucle

Pruebo con asignación

- r debe disminuir (es la cota).
- Despejar **E** y **k** de

$$\begin{array}{c}\{I \wedge B\} \\ q, r := \mathbf{E}, r - \mathbf{k} \\ \{I\}\end{array}$$

con $\mathbf{k} > 0$.

$=$ Encontrar **E** y **k** tal que

$$I \wedge B \Rightarrow wp.(q, r := \mathbf{E}, r - \mathbf{k}).I$$

sea verdadera.

$=$ Suponer $I \wedge B$ y encontrar **E** y **k** tal que

$$wp.(q, r := \mathbf{E}, r - \mathbf{k}).I$$

sea verdadera.

5. Cuerpo del bucle

Programa anotado a derivar

Var $x, y, q, r : Int$;
$\{P : x \geq 0 \ \wedge \ y > 0\}$
$q,r := 0, x;$ $\heartsuit$
$\{I : x = q * y + r \ \wedge \ 0 \leq r\}$
do $r \geq y \ \rightarrow$
  $\{I \ \wedge \ B\}$
  q,r := **E**, r - **k** ?
  $\{I\}$
od
$\{I \ \wedge \ \neg B : x = q * y + r \ \wedge \ 0 \leq r \ \wedge \ r < y\}$ $\heartsuit$
$\{Q : x = q * y + r \ \wedge \ 0 \leq r \ \wedge \ r < y\}$

5. Cuerpo del bucle

Derivación

5. Cuerpo del bucle

Derivación

Sup $I \wedge B : x = q * y + r \wedge 0 \leq r \wedge r \geq y$

$wp.(q, r := \mathbf{E}, r - \mathbf{k}).(x = q * y + r \wedge 0 \leq r)$

5. Cuerpo del bucle

Derivación

Sup $I \wedge B : x = q * y + r \wedge 0 \leq r \wedge r \geq y$

$$
\begin{aligned}
& wp.(q, r := \mathbf{E}, r - \mathbf{k}).(x = q * y + r \wedge 0 \leq r) \\
\equiv\ & \{ \text{ Def } wp \ \} \\
& x = \mathbf{E} * y + (r - \mathbf{k}) \wedge 0 \leq r - \mathbf{k}
\end{aligned}
$$

5. Cuerpo del bucle

Derivación

Sup $I \wedge B : x = q * y + r \wedge 0 \leq r \wedge r \geq y$

$$
\begin{aligned}
& wp.(q, r := \mathbf{E}, r - \mathbf{k}).(x = q * y + r \wedge 0 \leq r) \\
\equiv \; & \{ \text{ Def } wp \text{ } \} \\
& x = \mathbf{E} * y + (r - \mathbf{k}) \wedge 0 \leq r - \mathbf{k} \\
\equiv \; & \{ \text{ Sup. } x = q * y + r \text{ } \} \\
& q * y + r = \mathbf{E} * y + r - \mathbf{k} \wedge 0 \leq r - \mathbf{k}
\end{aligned}
$$

5. Cuerpo del bucle

Derivación

Sup $I \wedge B : x = q * y + r \wedge 0 \leq r \wedge r \geq y$

$$
\begin{aligned}
& wp.(q, r := \mathbf{E}, r - \mathbf{k}).(x = q * y + r \wedge 0 \leq r) \\
\equiv\ & \{ \text{ Def } wp \ \} \\
& x = \mathbf{E} * y + (r - \mathbf{k}) \wedge 0 \leq r - \mathbf{k} \\
\equiv\ & \{ \text{ Sup. } x = q * y + r \ \} \\
& q * y + r = \mathbf{E} * y + r - \mathbf{k} \wedge 0 \leq r - \mathbf{k} \\
\equiv\ & \{ \text{ Aritmética } \} \\
& \mathbf{E} = q + \frac{\mathbf{k}}{y} \wedge \mathbf{k} \leq r
\end{aligned}
$$

5. Cuerpo del bucle

Derivación

Sup $I \wedge B : x = q * y + r \wedge 0 \leq r \wedge r \geq y$

$$
\begin{aligned}
& wp.(q, r := \mathbf{E}, r - \mathbf{k}).(x = q * y + r \wedge 0 \leq r) \\
\equiv \; & \{ \text{ Def } wp \text{ } \} \\
& x = \mathbf{E} * y + (r - \mathbf{k}) \wedge 0 \leq r - \mathbf{k} \\
\equiv \; & \{ \text{ Sup. } x = q * y + r \text{ } \} \\
& q * y + r = \mathbf{E} * y + r - \mathbf{k} \wedge 0 \leq r - \mathbf{k} \\
\equiv \; & \{ \text{ Aritmética } \} \\
& \mathbf{E} = q + \tfrac{\mathbf{k}}{y} \wedge \mathbf{k} \leq r \\
\equiv \; & \{ \text{ Elegimos } \mathbf{k} \leftarrow y\text{, menor múltiplo positivo de y } \} \\
& \mathbf{E} = q + \tfrac{y}{y} \wedge y \leq r
\end{aligned}
$$

5. Cuerpo del bucle

Derivación

Sup $I \wedge B : x = q * y + r \wedge 0 \leq r \wedge r \geq y$

$$
\begin{array}{ll}
 & wp.(q, r := \mathbf{E}, r - \mathbf{k}).(x = q * y + r \wedge 0 \leq r) \\
\equiv & \{ \text{ Def } wp \text{ } \} \\
 & x = \mathbf{E} * y + (r - \mathbf{k}) \wedge 0 \leq r - \mathbf{k} \\
\equiv & \{ \text{ Sup. } x = q * y + r \text{ } \} \\
 & q * y + r = \mathbf{E} * y + r - \mathbf{k} \wedge 0 \leq r - \mathbf{k} \\
\equiv & \{ \text{ Aritmética } \} \\
 & \mathbf{E} = q + \frac{\mathbf{k}}{y} \wedge \mathbf{k} \leq r \\
\equiv & \{ \text{ Elegimos } \mathbf{k} \leftarrow y \text{, menor múltiplo positivo de y } \} \\
 & \mathbf{E} = q + \frac{y}{y} \wedge y \leq r \\
\equiv & \{ \text{ Aritmética y sup. } B \text{ } \} \\
 & \mathbf{E} = q + 1
\end{array}
$$

5. Cuerpo del bucle

Derivación

Sup $I \wedge B : x = q * y + r \wedge 0 \leq r \wedge r \geq y$

$$
\begin{array}{ll}
 & wp.(q, r := \mathbf{E}, r - \mathbf{k}).(x = q * y + r \wedge 0 \leq r) \\
\equiv & \{ \text{ Def } wp \text{ } \} \\
 & x = \mathbf{E} * y + (r - \mathbf{k}) \wedge 0 \leq r - \mathbf{k} \\
\equiv & \{ \text{ Sup. } x = q * y + r \text{ } \} \\
 & q * y + r = \mathbf{E} * y + r - \mathbf{k} \wedge 0 \leq r - \mathbf{k} \\
\equiv & \{ \text{ Aritmética } \} \\
 & \mathbf{E} = q + \frac{\mathbf{k}}{y} \wedge \mathbf{k} \leq r \\
\equiv & \{ \text{ Elegimos } \mathbf{k} \leftarrow y \text{, menor múltiplo positivo de y } \} \\
 & \mathbf{E} = q + \frac{y}{y} \wedge y \leq r \\
\equiv & \{ \text{ Aritmética y sup. } B \text{ } \} \\
 & \mathbf{E} = q + 1 \\
\equiv & \{ \text{ Hacemos } \mathbf{E} \leftarrow q + 1 \text{ } \} \\
 & \mathit{True}
\end{array}
$$

5. Cuerpo del bucle

Programa anotado correcto parcialmente

Var $x, y, q, r : Int$;
$\{P : x \geq 0 \wedge y > 0\}$
q,r := $0, x$; ♡
$\{I : x = q * y + r \wedge 0 \leq r\}$
do $r \geq y \rightarrow$
  $\{I \wedge B\}$
  q,r := q+1, r - y ♡
  $\{I\}$
od
$\{I \wedge \neg B : x = q * y + r \wedge 0 \leq r \wedge r < y\}$ ♡
$\{Q : x = q * y + r \wedge 0 \leq r \wedge r < y\}$

Programa correcto parcialmente

Var $x, y, q, r : Int$;
q,$r := 0, x$;
do $r \geq y \rightarrow$
  q,r := q+1, r - y
od

Programa correcto parcialmente

Var $x, y, q, r : Int$;
q,$r := 0, x$;
do $r \geq y \rightarrow$
  q,r := q+1, r - y
od

Falta demostrar terminación

6. Cota positiva $I \wedge B \Rightarrow t \geq 0$

- Hay que demostrar la implicación

$$I \wedge B \Rightarrow r \geq 0$$

6. Cota positiva $I \wedge B \Rightarrow t \geq 0$

- Hay que demostrar la implicación

$$I \wedge B \Rightarrow r \geq 0$$

- Supongo $I \wedge B$ y tengo que hacer *True* a $r \geq 0$.

6. Cota positiva $I \wedge B \Rightarrow t \geq 0$

- Hay que demostrar la implicación

$$I \wedge B \Rightarrow r \geq 0$$

- Supongo $I \wedge B$ y tengo que hacer *True* a $r \geq 0$.

Demostración

Sup $I \wedge B : x = q * y + r \wedge 0 \leq r \wedge r \geq y$

$$\begin{array}{ll} & r \geq 0 \\ \equiv & \{ \text{ Sup. } \} \\ & \mathit{True} \end{array}$$

Cota disminuye $\{I \wedge B \wedge t = T\}\ S\ \{t < T\}$

- Hay que demostrar la implicación

$$I \wedge B \wedge r = T \Rightarrow wp.(q, r := q + 1, r - y).(r < T)$$

Cota disminuye $\{I \wedge B \wedge t = T\}\ S\ \{t < T\}$

- Hay que demostrar la implicación

$$I \wedge B \wedge r = T \Rightarrow wp.(q, r := q + 1, r - y).(r < T)$$

- Supongo $I \wedge B \wedge r = T$ y tengo que hacer *True* a $wp.(q, r := q + 1, r - y).(r < T)$.

Cota disminuye $\{I \wedge B \wedge t = T\}\ S\ \{t < T\}$

- Hay que demostrar la implicación

$$I \wedge B \wedge r = T \Rightarrow wp.(q, r := q + 1, r - y).(r < T)$$

- Supongo $I \wedge B \wedge r = T$ y tengo que hacer *True* a $wp.(q, r := q + 1, r - y).(r < T)$.

Ejercicio

Sup $x = q * y + r \wedge 0 \leq r \wedge r \geq y \wedge r = T$

$$\begin{array}{ll} & wp.(q, r := q + 1, r - y).(r < T) \\ \equiv & \{\ \cdots\ \} \\ & \ldots \\ \equiv & \{\ \cdots\ \} \\ & \textit{True} \end{array}$$