$a, b \in \mathbb{Z}, \quad m, h \in \mathbb{Z}^+$

Probar que

$a \equiv b \pmod{m} \Leftrightarrow \exists i : 0 \leq i < h, \ a \equiv b + mi \pmod{mh}$

Ideas

R: $0 \leq i < h$ me hace acordar al resto de la división

F: expresar los enunciados con la definición de congruencia

Obs: hay que probar $(\Rightarrow)$ y $(\Leftarrow)$

$(\Leftarrow)$

$(\Leftarrow)$ $\exists i : 0 \leq i < h$, tal que $a \equiv b + mi \pmod{mh}$

por definición de $\equiv$, $\exists k$: (*) $a = m\underbrace{h \cdot k}\, + r \quad 0 \leq r < mh$

$b + mi = mh \cdot k' + r$ (1)

$b = -mi + mh \cdot k' + r = m\underbrace{(-i + hk')} + r$ (2)

r no necesariamente es el resto mód m, porque no necesariamente es $r < m$

No nos va a importar, porque al hacer congruencias no siempre hay que comparar un número con el resto

(*) Al pasar a igualdades entre números enteros "nos libramos" de la congruencia (m ó mh quedan multiplicados). Agregamos variables.

① $a \equiv r \pmod{m}$
② $b \equiv r \pmod{m}$

$$\left.\begin{array}{l} a \equiv r \pmod{m} \\ b \equiv r \pmod{m} \end{array}\right\} \Rightarrow a \equiv b \pmod{m}$$

Después que hicimos esta demostración,

F: podríamos haber hecho directamente $a \equiv b \pmod{m}$ probando que $a-b$ es múltiplo de m (no hace falta comparar siempre con el resto)

Directamente $a \equiv b + mi \pmod{mh}$

por def. $a - (b + mi) = mh \cdot K$

$a - b = mi + mh \cdot K = m(i + hK) = \dot{m}$

por def. $a \equiv b \mod (m)$

($\Rightarrow$) Partimos de que $a \equiv b \pmod{m}$

$a \equiv b + mi \pmod{m}$ (falta h)

congruencia mód mh "da más información" que congruencia mód m

Ideas

(división entera)

$a = mh \cdot k + r \quad , \; 0 \leq r < mh \rightsquigarrow 0 \leq \underbrace{\frac{r}{m}}_{\text{puede no ser entero.}} < h$

$a \equiv r \pmod{mh}$

$a = m \cdot l + s \quad , \; 0 \leq s < m$

$mh \cdot k + r = m \cdot l + s$

$r - s = ml - mhk = m\underbrace{(l - hk)}_{q}$

(recordemos que podemos hacer div. entera)

$r \equiv s \pmod{m}$

$G: \; r = mq + s$

Sustituimos

$$a = mhk + mq + s = m(\overset{\ell}{\overbrace{hk + q}}) + s$$

$a \equiv s \pmod{m}$ (ya lo sabíamos)

Recordar el objetivo:

Encontrar i : $0 \leq i \leq h$, $a \equiv b + mi \pmod{mh}$

$\rightarrow a - (b + mi) = mh \cdot q \Leftrightarrow$ por def

$a = m \cdot \ell + s$

$b = m\ell' + s$

es el mismo s porque $a \equiv b \pmod{m}$

$a - (b + mi) = m\ell + s - m\ell' - s - mi =$ me gustaría mhq

$m(\ell - \ell' - i) =$

$a-b = mk)$ porque $a \equiv b \pmod m$

$a-b = mh \cdot k' + r \quad 0 \leq r < mh$

demostraremos que $\exists i : r = mi$

$0 \leq k < h \quad 0 \leq i < h \qquad h \leq k < 2h$

Si $mh > a-b \geq 0$, $k' = 0$, $a-b = r$

mk

pero $a-b = mk$

(entonces $i = k$ sirve)

$q < h$

$h \leq q$

$h \leq k-h$

$2h \leq k$

Si $mh \leq a-b$ $\quad k = h + q \quad (k' = 1)$

también

tomo

Si $h > q \Rightarrow i = q \quad mh + mi = mk = (a-b)$

k

$2h \leq k$

Si $h \leq q \Rightarrow$ tomo $i = q - h$ estamos comparando q

con múltiplos de h

$q - h < h$

Va de nuevo la hoja anterior, más ordenada.

$a-b = mk$ porque $a \equiv b \pmod{m}$

$a-b = mh \cdot k' + r$ (división entera de $a-b$ entre mh)

$0 \leq r < mh$

Queremos llegar a que $\exists i : 0 \leq i < h : r = mi$

porque en este caso $a-(b+mi) = a-b-r = mh \cdot k'$

Separamos casos

I $a-b \geq 0$

II $a-b < 0$ → pero es lo mismo que resolver I con $b-a$

de este comentario concluimos que alcanza con resolver I

I Separamos casos

1 $mh > a-b \geq 0$

2 $mh \leq a-b$

① $0 \leq a-b < mh \Rightarrow$ es el resto

$ \overset{\shortparallel}{mk} < mh$

Entonces $a-b = mh \cdot 0 + a-b$

$= mh \cdot 0 + mk \quad = mk$

Podemos tomar $i = k$, porque $0 \leq mk < mh$

$a-b = mi$, $a = b + mi$ $\qquad \Rightarrow 0 \leq k < h$

$\Rightarrow a \equiv b + mi \ (mh)$

② $\overset{a-b}{\overset{\shortparallel}{mk}} \geq mh$, defino $q = k-h \geq 0$, $k = h + \underset{\geq 0}{q}$

$a-b = mh + mq$

Separamos en casos

$\boxed{2.1}$ $h > q$

$\boxed{2.2}$ $h \leq q$

$\boxed{2.1}$ $q < h$

Podemos tomar $i = q$

$$a - b = mh + mq \Rightarrow a - (b + mq) = mh$$

$$\Rightarrow a \equiv b + mq \pmod{mh}$$

$\boxed{2.2}$ $q \geq h$, $\quad q = h \cdot l + i$ (división entera)

$$0 \leq i < h$$

$$a - b = mk = m(h + q) = mh + mq$$

$$= mh + m(hl + i) = mh + mhl + mi$$

$$= mh(1 + l) + mi$$

$$a - (b + mi) = mh \cdot (1 + l) = \dot{m}h \Rightarrow a \equiv b + mi \pmod{mh}$$

También podríamos haber dividido directamente k entre h (nos dimos cuenta después)

$k = h \cdot p + i$

1. $p = 0$

$\boxed{2.1}$ $p = 1$

$a - b = mk$ $\boxed{2.2}$ $p \geq 2$

división entera (i es el resto)

$k = i + hk'$

con $0 \leq i < h$ (letra)

Salimos de $\underline{a = b + mk}$

Queremos llegar a $a = b + mi + mh \cdot k' = b + \underline{m(i + h \cdot k')}$

$a - b - mi = mhk'$