Sean $a, b, c, d$ tales que $(ad-bc) \mid a$, $(ad-bc) \mid c$

Probar que $mcd(an+b, cn+d) = 1 \quad \forall n \in \mathbb{N}$

Si no sabemos por dónde arrancar, escribimos los datos del problema según su definición.

$(ad-bc) \mid a$ ¿qué quiere decir?

que existe $q \in \mathbb{Z}$ tal que $a = (ad-bc)q$

$(ad-bc) \mid c \Rightarrow \exists\ q' \in \mathbb{Z}$ tal que $c = (ad-bc)q'$

$a = (ad-bc)q$ , $c = (ad-bc)q'$

$a = adq - bcq$ | $c = adq' - bcq'$

$a - adq = -bcq$ | $c + bcq' = adq'$

$a(1-dq) = c(-bq)$ | $c(1+bq') = a(dq')$

$1-dq \neq 0$

$dq' \neq 0$

$c \neq 0$

$mcd(q,q') = 1$

$mcd(q,b) = 1$

$mcd(q',d) = 1$

$\Rightarrow 1 + bq' - dq = 0$

$1 = -bq' + dq$

$= (-q')b + qd$

$\Downarrow$

$mcd(b,d) = 1$

Hagamos algo en $\mathbb{R}$ (o en $\mathbb{R}$)

$$a = c\,\frac{(-bq)}{1-dq} = c\,\frac{(1+bq')}{dq'}$$

chequear que estamos haciendo las cosas bien

$$(-bq)dq' = (1-dq)(1+bq') = 1 + bq' - dq - dqbq'$$

¿Si podemos relacionar $mcd(b,d)$ con $mcd(an+b, cn+d)$?

↳ pistas: que vale para $n=0$

Deducimos que $mcd(b,d)=1$

porque encontramos una combinación lineal entera de $b$ y $d$ que da 1: $1=(-q)b+qd$

¿Será que podemos hacer lo mismo con $an+b$ y $cn+d$?

$$a = ad q - bc q \quad | \quad c = ad q' - bc q'$$

$$a = (-cq)b + (aq)d \qquad c = (-cq')b + (aq')d$$

$$an = -cqnb + aqnd \qquad cn = -cq'nb + aq'nd$$

$$= (ad - bc)qn \qquad cn = (ad - bc)q'n$$

$$mcd(q, q') = 1$$

$$-q'b + qd = 1$$

$$-q'a + qc = -q'(adq - bcq) + q(adq' - bcq')$$

$$= -q'adq + q'bcq + adqq' - bcqq' = 0$$

$$a = (ad-bc)q \quad , \quad c = (ad-bc)q'$$

$$ad = (ad-bc)qd \quad , \quad bc = (ad-bc)q'b$$

$$ad-bc = (ad-bc)qd - (ad-bc)q'b$$

$$= (ad-bc)(qd-q'b)$$

$ad-bc = 0$

$qd-q'b = 1$

$\Updownarrow$

$mcd(b,d) = 1$

$(ad-bc) \mid a$ , $(ad-bc) \mid c$ , $(ad-bc)$ es un divisor común de $a$ y $c$

entonces $(ad-bc) \mid mcd(a,c)$ ⊕

$ad-bc$ es una combinación lineal de $a$ y $c$

$\Rightarrow mcd(a,c) \mid (ad-bc)$ ⊕

$mcd(a,c) = ad-bc$.

$mcd(b,d) = 1$

$1 = -q'b + qd$

$ad-bc$ es comb. lin. de $b$ y $d$

$mcd(b,d) \mid (ad-bc)$

$M = mcd(an+b, cn+d) \mid an+b$

$M = mcd(an+b, cn+d) \mid cn+d$

Queremos probar que $M = 1$

$M \mid (an+b)c = anc + bc$

$M \mid (cn+d)a = cna + ad$

$M \mid ad - bc = mcd(a, c)$

Buscar $x, y$ tales que

$$1 = x(an+b) + y(cn+d)$$

$$-q'b + qd = 1 \quad \checkmark$$

Probé $\quad -q'a + qc = 0$ (milagro de cuentas)

$$-q'b + qd + n(-q'a + qc) = 1 + n \cdot 0 = 1$$

$$= -q'(an+b) + q(cn+d)$$

Resumen de una buena redacción de la solución. (o sea, pasarla en limpio)

① $a = (ad-bc)q$, $c = (ad-bc)q'$
(definición de "dividir")

② (cuentas oportunas) $\Rightarrow -q'b + qd = 1$
completar y chequear.

③ (iluminación por haber mirado tanto el problema) $\Rightarrow -q'a + qc = 0$
completar

④ $-q'(an+b) + q(cn+d) = (-q'b+qd) + n(-q'a+qc) = 1+n\cdot 0 = 1$

⑤ encontramos comb. lin. de $an+b$ y $cn+d$ que da 1 $\Rightarrow \mathrm{mcd}(an+b, cn+d) = 1$