__/__/__ S T Q Q S S D

Assim, temos que:

$a - b = qk_2 - pk_1 \Rightarrow$ combinação linear de p e q

$\Rightarrow$ múltiplo do $mdc(p,q) \Rightarrow k' \, mdc(p,q)$

$\Rightarrow mdc(p,q) \mid a - b$

A ida ($\rightarrow$) está provada

Prova: ($\leftarrow$) Volta

Suponho que $mdc(p,q) \mid a - b$. Isso significa que:

$a - b = k \cdot mdc(p,q) \Rightarrow$

$\Rightarrow k(pu + qv)$ onde $u, v \in N$

Temos que isso é igual a: $pu' + qv'$ Onde: $u' = ku$
$v' = kv$

Agora, a próxima coisa que queremos notar é que temos um:

$x = a - pu' = b + qv'$

Podemos notar que isso significa que se reduzirmos o módulo p, obtemos que x é congruente com um mod p.