3.7.24. *a) Dar una condición necesaria y suficiente para que la progresión aritmética $an + b$ tenga infinitos cuadrados.*

b) Utilizar el apartado anterior para estudiar la existencia de infinitos cuadrados en la progresión $160 + 103n$.

a) Observamos que $an + b \equiv b \pmod{a}$.

Si en la progresión hay infinitos cuadrados, entonces $b \equiv x^2 \pmod{a}$ tiene solución. Recíprocamente, si $x^2 \equiv b \pmod{a}$ tiene solución, ésta será módulo a, luego existirán infinitos cuadrados en la sucesión. De hecho, si queremos un cálculo explícito, sea x_0^2 un cuadrado de la sucesión, entonces $x_0^2 \cdot (a+1)^{2n}$ también lo será para todo n natural.

Con todo esto hemos visto que una condición necesaria y suficiente para que $an + b$ tenga infinitos cuadrados es:

$$an + b = x^2 \equiv b \ (mod\ a)$$

$$\binom{b}{a} = 1$$

b) Veremos si se satisface $\binom{160}{103} = 1$.

$$\binom{160}{103} = 1 = \binom{57}{103} = \binom{19}{103}\binom{3}{103}$$

Ahora utilizamos la Ley de Reciprocidad Cuadrática:

$$\binom{19}{103}\binom{3}{103} = \binom{103}{19}(-1)^{\frac{(103-1)\cdot(19-1)}{4}}\binom{103}{3}(-1)^{\frac{(103-1)\cdot(3-1)}{4}} = \binom{103}{19}\binom{103}{3}$$

Y ahora simplificamos:

$$\binom{103}{19}\binom{103}{3} = \binom{8}{19}\binom{1}{3}$$

Sabemos que 1 es un residuo cuadrático módulo p $\Longrightarrow \binom{1}{3} = 1$
Utilizando la Prop. 3.6.7, $\binom{8}{19} = \binom{2}{19}^3 = -1$, ya que $19 \equiv 3 \pmod{8}$.

Con todo esto tenemos

$$\binom{160}{103} = -1$$

Y, por tanto, no hay infinitos cuadrados en la secesión $160 + 102n$.

Problema escrito por Jesús de los Nietos Valle.