3.7.25. *Dar una condición necesaria y suficiente, en función de a, b y c, para que la congruencia $ax^2 + bx + c \equiv 0 \pmod{p}$ tenga solución. Aplicar esto último para estudiar la existencia de soluciones de la congruencia $5x^2 - 13x + 8 \equiv 0 \pmod{37}$*

Solución: Queremos hallar una condición necesaria y suficiente para que la congruencia $ax^2 + bx + c \equiv 0 \pmod{p}$ tenga solución. Supongamos que $a \not\equiv 0 \pmod{p}$. En otro caso, la ecuación $bx + c = 0 \pmod{p}$ tiene solución si y sólo si $b \neq 0 \pmod{p}$.

Ahora, multiplicamos a ambos lados por $4a$:

$$(4a)\cdot(ax^2+bx+c) \equiv (4a^2)x^2+4abx+4ac \equiv (2a)^2x^2+4ab+4ac \equiv 0 \pmod{p}$$

Sumamos y restamos b^2, y obtenemos:

$$(2a)^2x^2 + 4ab + b^2 - b^2 + 4ac \equiv (2ax + b)^2 + 4ac - b^2 \equiv 0 \pmod{p} \iff$$

$$\iff (2ax + b)^2 = b^2 - 4ac \pmod{p}$$

Al ser $a \not\equiv 0 \pmod{p}$, la ecuación $2ax + b \equiv y \pmod{p}$ tiene solución. Por lo que obtenemos que, llamando $y = 2ax + b$, hallamos que la ecuación $ax^2 + bx + c \equiv 0 \pmod{p}$ tiene solución si y slo si $y^2 = b^2 - 4ac \pmod{p}$ tiene solución. Es decir, si $b^2 - 4ac$ es un residuo cuadrático módulo p o $b^2 - 4ac \equiv 0 \pmod{p}$, entonces, la ecuación tiene solución, y viceversa.

Ahora, estudiemos si la ecuación $5x^2 - 13x + 8 \equiv 0 \pmod{37}$ tiene solución. $b^2 - 4ac = 169 - 4 \cdot 5 \cdot 8 = 169 - 160 = 9$

Como $9 \pmod{37} = 3^2 \pmod{37}$, la ecuación tiene solución.

Problema escrito por Javier Sanz-Cruzado Puig