Exercici 39. Calculeu totes les solucions de la congruència:
$x^2 + 6x - 31 \equiv 0 \pmod{72}$.

Resolució: $x^2 + 6x - 31 \equiv 0 \pmod{72}$. Primer, veiem que 72 no és un nombre primer, però $\mathbb{Z}/72\mathbb{Z} \cong \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z}$, aixi que reescribim la equació com un sistema de congruències:
$\begin{cases} x^2 + 6x - 31 \equiv 0 \pmod{2^3} \\ x^2 + 6x - 31 \equiv 0 \pmod{3^2} \end{cases}$
Ara tractarem cada cas per separat.

Usarem aquest algorisme, que és molt més pulit que la fòrmula quadràtica:

MÈTODE PER RESOLDRE CONGRUÈNCIES QUADRÀTIQUES

Per resoldre la congruència $ax^2 + bx + c \equiv 0 \pmod{p^n}$:

(i) Multipliquem al congruència per $4a$: $4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p^n}$

(ii) Reescribim la expressió com $(2ax + b)^2 \equiv b^2 - 4ac \pmod{p^n}$

(iii) Trobem les arrels de $b^2 - 4ac \pmod{p^n}$

(iv) Per cada arrel r_i, resolem la congruència lineal $2ax + b \equiv r \pmod{p^n}$

(v) Revisar si hi ha alguna solució que no funcioni.

- primitive roots
- solving quadratic congruences

Observació: Fem notar que l'algorisme que usarem és molt similar a la fòrmula quadràtica, però serà més fàcil buscar les arrels així. Usant la fòrmula quadràtica obtindriem els mateixos resultats.

(i) $x^2 + 6x - 31 \equiv x^2 + 6x + 1 \equiv 0 \pmod{2^3}$
Multipliquem per 4 la congruència:
$4x^2 + (4)(6)x + 4 \equiv 0 \pmod{2^3}$
Reescribim la congruència:
$(2x + 6)^2 \equiv 6^2 - 4 \pmod{2^3}$
Les arrels $y^2 \equiv 6^2 - 4 \equiv 32 \equiv 0 \pmod{2^3}$ és una unica arrel $r = 0$.
Resolem la congruència lineal $2x + 6 \equiv 0 \pmod{2^3} \implies x = 1 \; i \; x = 5$.
$x_i = \{1, 5\}$

(ii) $x^2 + 6x - 31 \equiv x^2 + 6x + 5 \equiv 0 \pmod{3^2}$
Multipliquem per 4 la congruència:
$4x^2 + (4)(6)x + (4)(5) \equiv 0 \pmod{3^2}$
Reescribim la congruència:
$(2x + 6)^2 \equiv 6^2 - (4)(5) \pmod{3^2}$
Les arrels $y^2 \equiv 6^2 - (4)(5) \equiv 7 \pmod{3^2}$ són $r_0 = 4$ i $r_1 = 5$.
Resolem la congruència lineal $2x + 6 \equiv r_0, r_1 \pmod{3^2} \implies x = 8 \; i \; x = 4$.
$y_i = \{8, 4\}$

Finalment, hem de resoldre 4 sistemes pel TXR: $r_k = \{x_i, y_j\}, i, j \in \{1, 2\}$

$r_1 = \{1, 8\} \quad m = \{2^3, 3^2\} \quad x \equiv 17 \pmod{72}$
$r_2 = \{1, 4\} \quad m = \{2^3, 3^2\} \quad x \equiv 49 \pmod{72}$
$r_3 = \{5, 4\} \quad m = \{2^3, 3^2\} \quad x \equiv 13 \pmod{72}$
$r_4 = \{5, 8\} \quad m = \{2^3, 3^2\} \quad x \equiv 53 \pmod{72}$

Aquest sistema té les arrels $x = \{13, 17, 49, 53\}$.
