Congruències quadràtiques

Exercici 38. Calculeu totes les solucions de les congruències:

(i) $x^2 + x + 1 \equiv 0 \pmod 7$.

(ii) $x^2 + 5x + 1 \equiv 0 \pmod 7$.

(iii) $x^2 + 3x + 1 \equiv 0 \pmod 7$.

Resolució:

(i) $x^2 + x + 1 \equiv 0 \pmod 7$

Provem de resoldre la congruència mitjançant la fòrmula quadràtica $\dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.
$\dfrac{-1 \pm \sqrt{1-4}}{2} = \dfrac{-1 \pm \sqrt{-3}}{2}$. Primer hem de resoldre la congruència $y \equiv \sqrt{-3} \pmod 7$, que la podem reescriure com $y^2 \equiv -3 \equiv 4 \pmod 7$, que té les solucions $y = \pm 2$.
Ara veiem que dividir per 2 és el mateix multiplicar per la inversa de 2. En $\mathbb{Z}/7\mathbb{Z}$, la inversa de 2 és 4. Així doncs, hem de resoldre $(-1 \pm (\pm 2))(4) = \begin{cases} (-1+2)(4) \equiv 4 \pmod 7 \\ (-1-2)(4) \equiv 2 \pmod 7 \\ (-1+(-2))(4) \equiv 2 \pmod 7 \\ (-1-(-2))(4) \equiv 4 \pmod 7 \end{cases}$
Llavors, les solucions de $x^2 + x + 1 \equiv 0 \pmod 7$ són $x = 2, 4$.

(ii) $x^2 + 5x + 1 \equiv 0 \pmod 7$

Provem de resoldre la congruència mitjançant la fòrmula quadràtica $\dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.
$\dfrac{-5 \pm \sqrt{5^2 - 4}}{2} = \dfrac{-5 \pm \sqrt{21}}{2}$. Primer hem de resoldre la congruència $y \equiv \sqrt{21} \pmod 7$, que la podem reescriure com $y^2 \equiv 21 \equiv 0 \pmod 7$, que té les solucions $y = 0$.
Ara veiem que dividir per 2 és el mateix multiplicar per la inversa de 2. En $\mathbb{Z}/7\mathbb{Z}$, la inversa de 2 és 4. Així doncs, hem de resoldre $(-5 \pm (0))(4) = \{(-5)(4) \equiv 1 \pmod 7$
Llavors, la solució de $x^2 + 5x + 1 \equiv 0 \pmod 7$ és $x = 1$.

(iii) $x^2 + 3x + 1 \equiv 0 \pmod 7$

Provem de resoldre la congruència mitjançant la fòrmula quadràtica $\dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.
$\dfrac{-3 \pm \sqrt{3^2 - 4}}{2} = \dfrac{-3 \pm \sqrt{5}}{2}$. Primer hem de resoldre la congruència $y \equiv \sqrt{5} \pmod 7$, que la podem reescriure com $y^2 \equiv 5 \pmod 7$. Com no és immediat, mirem si té arrels amb el símbol de Legendre, usant el criteri d'Euler. $\left(\dfrac{5}{7}\right) \equiv 5^{\frac{7-1}{2}} \equiv 5^3 \equiv 125 \equiv -1 \pmod 7$. Així doncs $y^2 \equiv 5 \pmod 7$ no té solució, així doncs, $x^2 + 3x + 1 \equiv 0 \pmod 7$ no té solució.
