Given that 2 is a primitive element of \((\mathbb{Z}/37\mathbb{Z})^*\) find a primitive 3rd root of 1 in \(\mathbb{Z}/37\) and a square root of \(-3\) (hint: in \(\mathbb{C}\) let \(\zeta = \exp(2\pi i/3) = -1/2 + \sqrt{-3}/2\) be a primitive 3rd root of 1, then \(\zeta - \zeta^2 = \sqrt{-3}\)).

\[
2^5 = 32 = -5, 2^{10} = 25, 2^{12} = 100 = 26 \text{ is a primitive 3rd root of 1 in } \mathbb{Z}/37\mathbb{Z} \text{ (since } 12 = \frac{1}{3}(\mathbb{Z}/37\mathbb{Z})^*). \\
\text{Let } \zeta = 26 = -11 \text{ then } \zeta^2 = 121 = 10 \text{ so } \zeta - \zeta^2 = 16.
\]

Does \(X^2 - 6X + 15 = 0\) have a solution modulo 61?

Completing the square we get \((X - 3)^2 = -6\) and so we must check if \(-6\) is a square modulo 61. We have \((\frac{-6}{61}) = (\frac{-1}{61})(\frac{2}{61})(\frac{3}{61})\). Now \((\frac{-1}{61}) = 1\) as \(61 \equiv 1\), \((\frac{2}{61}) = -1\) as \(61 \equiv 5\). Since \(61 \equiv 1\), then \((\frac{3}{61}) = (\frac{61}{3}) = (\frac{1}{3}) = 1\) hence \((\frac{-6}{61}) = -1\) so \(-6\) is not a square modulo 61 and the equation can not be solved.