

Megoldás. Legyen ε_1 és ε_2 az $x^2 + x + 1$ polinom két komplex gyöke; ezek nem mások, mint az 1-től különböző harmadik egységgyökök. A polinom gyöktényezős alakja $(x - \varepsilon_1)(x - \varepsilon_2)$, ezért a binomiális tétel alapján

$$\begin{aligned} (x^2 + x + 1)^p &= (x - \varepsilon_1)^p (x - \varepsilon_2)^p = \\ &= \left(\sum_{k=0}^p (-1)^k \binom{p}{k} \varepsilon_1^k x^{p-k} \right) \left(\sum_{k=0}^p (-1)^k \binom{p}{k} \varepsilon_2^k x^{p-k} \right). \end{aligned}$$

A polinomban az x^p együtthatója:

$$\begin{aligned} a_p &= \sum_{k=0}^p (-1)^k \binom{p}{k} \varepsilon_1^k \cdot (-1)^{p-k} \binom{p}{p-k} \varepsilon_2^{p-k} = - \sum_{k=0}^{(p-1)/2} \binom{p}{k}^2 (\varepsilon_1^{p-2k} + \varepsilon_2^{p-2k}) = \\ &= -(\varepsilon_1^p + \varepsilon_2^p) - \sum_{k=1}^{(p-1)/2} \binom{p}{k}^2 (\varepsilon_1^{p-2k} + \varepsilon_2^{p-2k}). \end{aligned}$$

Tetszőleges u egész számra $\varepsilon_1^u + \varepsilon_2^u = 2$, ha u osztható 3-mal, és $\varepsilon_1^u + \varepsilon_2^u = -1$, ha u nem osztható 3-mal. Mivel p nem osztható 3-mal, $\varepsilon_1^p + \varepsilon_2^p = -1$. A $\binom{p}{k}$ binomiális együttható pedig $0 < k < p$ esetén mindig osztható p -vel. Ezért $a_p \equiv -(\varepsilon_1^p + \varepsilon_2^p) = 1 \pmod{p^2}$.

()

Több dolgozat alapján