When a quartic has two irreducible quadratic factors

Anmol Sahu · 28 November 2026

Abstract

Translation turns the polynomial into the fifth cyclotomic polynomial. Raising its roots to the pth power permutes them, and the lengths of the cycles are the factor degrees.

Statement

For each prime p, work with polynomial coefficients modulo p. Let F(X) be the polynomial quotient $((X+1)^5-1)/X$. It has exactly two distinct monic irreducible quadratic factors if and only if p has remainder 9 upon division by 10. Monic means that the leading coefficient is one, and irreducible means that there is no factorization into lower-degree nonconstant polynomials over the same field. [1]

Proof

Write $G(Y) = 1 + Y + Y^2 + Y^3 + Y^4$. The geometric-sum identity gives $F(X) = G(X+1)$. Substitution by $X+1$ and its inverse $X-1$ preserve degrees, products and monicity. We may therefore factor G instead. For $p = 5$ the binomial theorem gives $F(X) = X^4$, which has no irreducible quadratic factor.

Suppose p differs from 5. The five roots of $Y^5 = 1$ are distinct, because the derivative $5Y^4$ is nonzero at each. Apart from 1 they all have multiplicative order five, and they are precisely the four roots of G. For any one of them, say z, raising to the pth power repeatedly yields z, z^p, z raised to p^2, and so on. The first return after d steps occurs exactly when p raised to d is congruent to 1 modulo 5.

The product of Y minus each root in this cycle has coefficients fixed by the pth-power map, hence in the field of p elements. Conversely, any polynomial over that field vanishing at z vanishes at every root in the cycle. Thus its minimal polynomial has degree d. Each cycle has the same length d, so there are exactly two quadratic factors precisely when $d = 2$.

Among the nonzero residues modulo 5, only 4 has multiplicative order two: it is -1 modulo 5. A prime congruent to 4 modulo 5 must be odd, which makes its last digit 9. Conversely every prime ending in 9 is congruent to 4 modulo 5. [3]

Context and attribution

Warut Roonguthai contributed OEIS A030433. Federico Provvedi proposed the shifted criterion in OEIS A030433 in 2018. Jianing Song recorded the equivalent criterion for the unshifted polynomial in the same sequence in 2022. [1]

References

[1] OEIS A030433, comments by Federico Provvedi and Jianing Song
[2] Left to Solve · statement of the submitted problem
[3] Open Math Agents · merged proof, pull request #7813