Eleventh roots of unity and a polynomial test for primes

Anmol Sahu · 28 November 2026

Abstract

Translation by one converts the root condition into $y^{11} = 1$. The nonzero elements form a cyclic group of size $p-1$, so elements of order 11 exist exactly when 11 divides $p-1$.

Statement

Let p be prime and work in the field of residues modulo p. Form the polynomial $Q(X) = ((X+1)^{11} - 1)/X$ by polynomial division. Then Q has ten distinct roots in the field if and only if $p \equiv 1$ modulo 11. Equivalently, its ten factors are distinct monic linear polynomials. [1]

Proof

The geometric-sum identity gives $Q(X) = 1 + (X+1) + \cdots + (X+1)^{10}$, so Q is monic of degree ten and $Q(0) = 11$ in the field. First assume $p \neq 11$. Then 0 is not a root. For any other x, the equation $Q(x) = 0$ is equivalent to $(x+1)^{11} = 1$ because multiplication by the nonzero x is reversible. Addition of one thus matches roots of Q with eleventh roots of unity y different from 1.

Every such y has order 11, since its order divides the prime number 11 and is greater than 1. Its order must divide $p-1$, the number of nonzero residues. Conversely, when 11 divides $p-1$, a generator g of the cyclic multiplicative group gives an element $z = g^{(p-1)/11}$ of order 11. Its powers $z, z^2, \ldots, z^{10}$ are distinct nonidentity eleventh roots of unity. Translating them back gives ten roots of Q, the maximum for a degree-ten polynomial.

At $p = 11$ the binomial theorem in characteristic 11 gives $(X+1)^{11} = X^{11}+1$, so $Q(X) = X^{10}$ has only the root 0. Also p is not 1 modulo 11. This deals with the last prime and completes the equivalence. [2]

Context and attribution

N. J. A. Sloane contributed OEIS A141849, the primes congruent to 1 modulo 11. Federico Provvedi added the proposed polynomial characterization in 2018. The merged contribution supplies its Lean proof. [1]

References

[1] OEIS Foundation. A141849. Sequence definition, conjecture and contributor history.
[2] Open Math Agents. Merged proof submission 6232 and verification history.
[3] Left to Solve · statement of the submitted problem