A ring-theoretic lemma behind the Laurent–Underwood cubic test

(informal note prepared with GPT-5.2 Pro)

2026-01-17

Abstract

This short note isolates a purely algebraic equivalence that appears implicitly in the final step of the Laurent–Underwood (LU) "cubic composite test". It is designed to be easy to formalize in Lean: the proof uses only quotient-ring arithmetic and a unit-cancellation step.

1 Set-up

Fix an integer $N \geq 2$ and an integer q with $\gcd(N, q) = 1$. Let

$$f(x) = x^3 - qx - q \in (\mathbb{Z}/N\mathbb{Z})[x], \qquad R := (\mathbb{Z}/N\mathbb{Z})[x]/(f).$$

Write $\alpha \in R$ for the image of x. Thus the defining relation in R is

$$\alpha^3 = q\alpha + q. \tag{1}$$

Notation. We will use the two elements

$$B := \alpha^{N-1} \in R, \qquad Y := \alpha^N = \alpha B \in R.$$

(When N is prime and f is irreducible mod N, one interprets $Y = \alpha^N$ as the Frobenius image of α. Nothing in the present lemma uses that interpretation.)

2 A unit computation

Lemma 1 (A convenient inverse for α)**.** *In R one has*

$$\alpha(\alpha^2 - q) = q. \tag{2}$$

In particular α is a unit in R (because q is a unit in $\mathbb{Z}/N\mathbb{Z}$ under $\gcd(N, q) = 1$), and one may take

$$\alpha^{-1} = q^{-1}(\alpha^2 - q).$$

Proof. Using (**??**),

$$\alpha(\alpha^2 - q) = \alpha^3 - q\alpha = (q\alpha + q) - q\alpha = q.$$

Since $\gcd(N, q) = 1$, the class of q in $\mathbb{Z}/N\mathbb{Z}$ is invertible, hence so is α. □

3 The LU congruence versus a quadratic identity

The LU final check (in their notation with $a = q$) compares $B^2 + B + 1$ against the quadratic polynomial $-x^2 + x + q$ modulo (N, f). In our ring-theoretic language this is the equation

$$B^2 + B + 1 = -\alpha^2 + \alpha + q \qquad \text{in } R. \tag{3}$$

Lemma 2 (Key equivalence)**.** *Assume* $\gcd(N, q) = 1$. *Then the LU final congruence* (**??**) *is equivalent to the quadratic identity*

$$Y^2 + \alpha Y + \alpha^2 = q \qquad \textit{in } R. \tag{4}$$

Proof. We prove the two implications.

(LU ⇒ quadratic in Y). Assume (**??**). Multiply both sides by α^2:

$$\alpha^2(B^2 + B + 1) = \alpha^2(-\alpha^2 + \alpha + q).$$

The left-hand side becomes, using $Y = \alpha B$,

$$\alpha^2(B^2 + B + 1) = (\alpha B)^2 + \alpha(\alpha B) + \alpha^2 = Y^2 + \alpha Y + \alpha^2.$$

For the right-hand side,

$$\alpha^2(-\alpha^2 + \alpha + q) = -\alpha^4 + \alpha^3 + q\alpha^2.$$

Using (**??**) we compute

$$\alpha^4 = \alpha\alpha^3 = \alpha(q\alpha + q) = q\alpha^2 + q\alpha,$$

so

$$-\alpha^4 + \alpha^3 + q\alpha^2 = -(q\alpha^2 + q\alpha) + (q\alpha + q) + q\alpha^2 = q.$$

Thus (**??**) holds.

(Quadratic in Y ⇒ LU). Assume (**??**). Reversing the above computation shows

$$\alpha^2(B^2 + B + 1) = \alpha^2(-\alpha^2 + \alpha + q).$$

By Lemma **??**, α is a unit in R, hence so is α^2, so we can cancel α^2 from both sides and obtain (**??**). □

4 Why this is a useful "Lean lemma"

Remark 1. *Lemma* **??** *is entirely internal to the quotient ring R. It uses only: (i) rewriting by the relation* $\alpha^3 = q\alpha + q$*; (ii) a unit-cancellation step justified by* $\gcd(N, q) = 1$.

In a Lean development, the only nontrivial "plumbing" is making the cancellation step explicit (typically via `IsUnit` *and* `mul_eq_mul_left_iff` */* `isUnit_mul_left_cancel` *lemmas).*