

# Mathematical Background

Jan-2026

## The Polynomial Remainder Theorem

We will develop the constructive proof briefly mentioned in the wikipedia article on [polynomial remainder theorem](#).

Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

be a polynomial with coefficients in a ring, and let  $r$  be any element of the ring. Then there exists a polynomial  $Q(x)$  of degree at most  $(n-1)$  such that

$$f(x) = (x - r) Q(x) + f(r).$$

The remainder of the division of  $f(x)$  by the linear polynomial  $(x - r)$  is exactly  $f(r)$ .

### Proof

#### The polynomial and its evaluation at $r$

Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0.$$

Evaluate  $f(r)$ :

$$f(r) = a_n r^n + a_{n-1} r^{n-1} + \dots + a_1 r + a_0.$$

#### The difference $f(x) - f(r)$

$$\begin{aligned} f(x) - f(r) &= (a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0) - (a_n r^n + a_{n-1} r^{n-1} + \dots + a_1 r + a_0). \\ &= (a_n x^n - a_n r^n) + (a_{n-1} x^{n-1} - a_{n-1} r^{n-1}) + \dots + (a_1 x - a_1 r) + (a_0 - a_0) \\ &= \underbrace{a_n(x^n - r^n)}_{\text{TERM } n} + \underbrace{a_{n-1}(x^{n-1} - r^{n-1})}_{\text{TERM } n-1} + \dots + \underbrace{a_1(x - r)}_{\text{TERM } 1} \end{aligned}$$

#### Recall the algebraic identity

$$\begin{aligned} x^k - r^k &= (x - r)(x^{k-1} + x^{k-2}r + \dots + xr^{k-2} + r^{k-1}) \quad \text{for an integer } k \geq 1. \\ a_k(x^k - r^k) &= a_k(x - r)(x^{k-1} + x^{k-2}r + \dots + xr^{k-2} + r^{k-1}) \quad \text{for } k = 1, \dots, n. \end{aligned}$$

**Apply the identity to each term in  $f(x) - f(r)$**

Consider the term  $a_n(x^n - r^n)$  in the above equation, and substitute

$$a_k(x^k - r^k) = (x - r) a_k(x^{k-1} + x^{k-2}r + \dots + r^{k-1}) \quad 1 \leq k \leq n.$$

Rewriting the terms in (5) gives

$$\begin{aligned} a_n(x^n - r^n) &= (x - r) a_n(x^{n-1} + x^{n-2}r + \dots + r^{n-1}) \\ a_n(x^{n-1} - r^{n-1}) &= (x - r) a_{n-1}(x^{n-2} + x^{n-3}r + \dots + r^{n-2}) \\ &\vdots \\ a_1(x - r) &= (x - r) a_1 \end{aligned}$$

**Factor out  $(x - r)$ .**

$$\begin{aligned} f(x) - f(r) &= (x - r) a_n(x^{n-1} + x^{n-2}r + \dots + r^{n-1}) \\ &\quad + (x - r) a_{n-1}(x^{n-2} + x^{n-3}r + \dots + r^{n-2}) \\ &\quad + \dots + (x - r) a_1. \end{aligned}$$

Factor  $(x - r)$  from the entire sum (the right-hand side expression):

$$f(x) - f(r) = (x - r) \left( a_n(x^{n-1} + x^{n-2}r + \dots + r^{n-1}) + \dots + a_1 \right).$$

**Define the polynomial  $Q(x)$  and Complete the Proof**

Let

$$Q(x) = a_n(x^{n-1} + x^{n-2}r + \dots + r^{n-1}) + a_{n-1}(x^{n-2} + x^{n-3}r + \dots + r^{n-2}) + \dots + a_1.$$

where

$$\deg(Q) \leq n - 1$$

We use polynomial  $Q$ , and write

$$f(x) - f(r) = (x - r) Q(x).$$

from which it follows that

$$f(x) = (x - r) Q(x) + f(r).$$

■