The Remainder Theorem

Theorem 3 (Remainder Theorem). If $f \in F[x]$, (where $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{F}_p$), and $a \in F$, then

$$\text{rem}(f, x-a) = f(a).$$

Theorem 4 (Factor Theorem). If $f(x) \in R[x]$ and $a \in R$, where $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C},$ or $\mathbb{F}_p$, then

$$x - a \,|\, f(x) \Leftrightarrow f(a) = 0.$$

Remarks. 1) The Factor Theorem shows that there is a close connection between:

linear factors of a polynomial $f(x)$, and
roots of a polynomial (i.e. solutions of $f(x) = 0$).

2) The Factor Theorem is due to Descartes (1596–1650). Moreover, D'Alembert (1717–1783) proved:

Corollary 1. A non-zero polynomial $f(x) \in F[x]$ of degree n has at most n roots in F.

Corollary 2. If f and $g \in F[x]$ are two polynomials of degree $\leq n$ such that

$$f(a_i) = g(a_i), \quad 1 \leq i \leq n+1,$$

for $n+1$ distinct elements $a_1, \ldots, a_{n+1}$, then $f = g$.

Corollary 3. Suppose that $f(x) \in F[x]$ and that $g(x)$ is a polynomial of the form

$$(1) \qquad g(x) = c(x - a_1)(x - a_2) \cdots (x - a_n)$$

with distinct roots $a_1, \ldots, a_n \in F$, i.e. $a_i \neq a_j$, for all $i \neq j$. Then $r(x) := \text{rem}(f, g)$ is the unique polynomial $r(x)$ of degree $\leq n - 1$ such that

$$(2) \qquad r(a_i) = f(a_i), \quad \text{for } 1 \leq i \leq n.$$

The Substitution Method for finding $\text{rem}(f, g)$:

Assume: $g(x)$ has the form (1) (with distinct a_i's).

Step 1: Write

$$\text{rem}(f, g) = r_0 + r_1 x + \ldots + r_{n-1} x^{n-1}.$$

Step 2: By (2), we have the following system of n linear equations in the unknowns $r_0, \ldots, r_{n-1}$:

$$\begin{aligned} r_0 + r_1 a_1 + \cdots + r_{n-1} a_1^{n-1} &= f(a_1) \\ &\vdots \\ r_0 + r_1 a_n + \cdots + r_{n-1} a_n^{n-1} &= f(a_n). \end{aligned}$$

Step 3: Solve this system (by row reduction and back-substitution) to find $r_0, \ldots, r_{n-1}$ and hence also $\text{rem}(f, g)$.