The Euclidean Algorithm

Definition: Let $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{F}_p$. A polynomial $h \in F[x]$ is called a common divisor of f and g if

$$h|_F f \quad \text{and} \quad h|_F g.$$

Moreover, h is called the greatest common divisor of f and g if:

1) h is a common divisor of f and g;

2) $\deg(h_1) \leq \deg(h)$ for all common divisors h_1 of f and g;

3) h is monic.

Notation: $h = \gcd(f, g)$. Unique! (as we shall see.)

Theorem 5 (Euclidean Algorithm). Let $f, g \in F[x]$.

a) The Euclidean algorithm computes the greatest common divisor $h = \gcd(f, g)$ of f and g up to a constant factor $c \neq 0$.

b) The method of back-substitution yields polynomials $k_1, k_2 \in F[x]$ such that

$$k_1 f + k_2 g = c \cdot h.$$

c) If h_1 is any common divisor of f and g, then $h_1 | h$.

Note: There is no Euclidean Algorithm for $\mathbb{Z}[x]$!