Theorem 2.4.4 (the Euclidean algorithm for polynomials)

Let $a, b \in F[x]$, $F$ a field, $a \neq 0$, $b \neq 0$.

Then $a$ and $b$ have a unique monic gcd $g \in F[x]$.

Moreover $\exists$ polynomials $\lambda, \mu \in F[x]$ s.t. $\lambda a + \mu b = g$.

Proof (existence of a gcd). Consider the sequence

$r_0 = a, r_1 = b, r_2, \dots, r_n, r_{n+1}$

$(a \div b) \quad a = b q_2 + r_2 \qquad \deg r_2 < \deg b$

$(b \div r_2) \quad b = r_2 q_3 + r_3 \qquad \deg r_3 < \deg r_2$

$\vdots$

$(r_{n-2} \div r_{n-1}) \quad r_{n-2} = r_{n-1} q_n + r_n \qquad \deg r_n < \deg r_{n-1}$

$(r_{n-1} \div r_n) \quad r_{n-1} = r_n q_{n+1} + r_{n+1} \qquad r_{n+1} = 0$

Claim $r_n | a$, $r_n | b$, and $c|a, c|b \Rightarrow c | r_n$.

Hence $g = lc(r_n)^{-1} r_n$ is a monic gcd of $a$ & $b$.

(uniqueness) Let $h$ be a gcd of $a$ & $b$ which is monic.

$\left.\begin{array}{l} g \text{ is a common divisor } \Rightarrow g|h \\ h \text{ is a common divisor } \Rightarrow h|g \end{array}\right\} \Rightarrow g = s \cdot h$ for $s \in F$.

But $lc(g) = lc(h) = 1 \Rightarrow s = 1 \Rightarrow g = h$.

(moreover) Let $\lambda_0 = 1, \lambda_1 = 0, \lambda_i = \lambda_{i-2} - \lambda_{i-1} \cdot q_i \quad 2 \le i \le n+1$

and $\mu_0 = 0, \mu_1 = 1, \mu_i = \mu_{i-2} - \mu_{i-1} \cdot q_i \quad 2 \le i \le n+1$

Claim $\lambda_i a + \mu_i b = r_i$ for $0 \le i \le n+1$.

Proof (by induction on $i$)

Hence $\lambda_n a + \mu_n b = r_n$. Let $s = lc(r_n)^{-1}$

$\underset{\times s}{\Rightarrow} \quad \underbrace{(s\lambda_n)}_{=\lambda} a + \underbrace{(s\mu_n)}_{=\mu} b = s \cdot r_n = g$