Theorem (Euclidean algorithm) Let $g(x)$ be a nonzero polynomial over a field $\mathbb{F}$. For every polynomial $f(x) \in \mathbb{F}[x]$, there exists a unique pair of polynomials $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that $f(x) = q(x)g(x) + r(x)$, with $\deg g > \deg r$ or $r(x)=0$.

Proof: If $f(x)=0$, then let $q(x)=r(x)=0$. In the following assume that $f(x) \neq 0$. Write $f(x) = a_n x^n + \dots + a_0$ and $g(x) = b_m x^m + \dots + b_0$, with $a_n \neq 0$, $b_m \neq 0$. We use induction on n. If $n<m$, then set $q(x)=0$ and $r(x)=f(x)$. It left to consider the case $n \geq m$. ~~If $n=m=0$, then set $q(x)=a_0b_0^{-1}$ and $r(x)=0$,~~

~~Now suppose that the theorem is true for all polynomials of degree~~

If $n=m$, then we have

$$f(x) = a_n b_m^{-1} g(x) + (f(x) - a_n b_m^{-1} g(x)),$$

where $f(x) - a_n b_m^{-1} g(x) = 0$ or $\deg(f(x) - a_n b_m^{-1} g(x)) < \deg f(x)$. Hence,

$$q(x) = a_n b_m^{-1}, \quad r(x) = f(x) - a_n b_m^{-1} g(x),$$

as required.

Now suppose that the theorem is true for all polynomials of degree $<n$ (where $n>m$). With this assumption, we write

$$f(x) = a_n b_m^{-1} x^{n-m} g(x) + f_1(x) \qquad (*)$$

where $f_1(x)=0$ or $\deg f_1(x) < \deg f(x)$. By the induction assumption, we find $q_1(x)$ and $r(x)$ for which

$$f_1(x) = q_1(x) g(x) + r(x), \quad \deg r(x) < \deg g(x) \text{ or } r(x)=0.$$

Substituting this into $(*)$ gives

$$f(x) = (q_1(x) + a_n b_m^{-1} x^{n-m}) g(x) + r(x).$$

~~Hence~~ Set $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$. Hence we obtain a pair of polynomials $q(x)$ and $r(x)$ with the required properties.

It remains to prove that $q(x)$ and $r(x)$ are unique (The same as we have talked in class). $\square$