Деление многочленов с остатком.

Пусть F - поле и $f(x), g(x) \in F[x]$ и $g(x) \neq 0$. Тогда $\exists!\ q(x), r(x) : f(x) = q(x) \cdot g(x) + r(x)$, при этом $\deg r(x) < \deg g(x)$.
$q(x)$ - частное
$r(x)$ - остаток

Доказательство

$$f(x) = a_k x^k + \cdots + a_0$$
$$g(x) = b_m x^m + \cdots + b_0$$

1. Докажем существование. В случае $k < m\ q(x) = 0$, а $r(x) = f(x)$. В случае $k \geq m$ докажем по индукции по $k - m$:
   1. База индукции: $k - m = 0$. Тогда $r(x) = f(x) - \frac{a_k}{b_k} g(x)$ и $q(x) = \frac{a_k}{b_k}$
   2. Шаг индукции: $k - m > 0$. Предположим, что теорема доказана для всех значений, меньших, чем $k - m$. Тогда возьмём $q(x) = \frac{a_k}{b_k} x^{k-m}$ и $h(x) = f(x) - \frac{a_k}{b_k} x^{k-m} g(x)$. Тогда $\deg h(x) < k$. Тогда для $h(x)$ воспользуемся предположением индукции. Тогда

$$f(x) = h(x) + \frac{a_k}{b_k} x^{k-m} g(x) =$$
$$= \frac{a_k}{b_m} x^{k-m} g(x) + q_1(x) g(x) + r_1(x) =$$
$$= (\frac{a_k}{b_m} x^{k-m} + q_1(x)) g(x) + r_1(x)$$

2. Единственность. Предположим, что есть два разложения:
   $f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$. Тогда

$$q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$$
$$q_1(x)g(x) - q_2(x)g(x) = r_2(x) - r_1(x)$$
$$(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x)) \quad *$$

   Если мы умножаем на $g(x) \neq 0$, то степень многочлена не уменьшается. Тогда если $q_1(x) \neq q_2(x)$, то в $(*)$ степени равных многочленов отличаются. Поэтому $(*)$ выполняется только если $q_1(x) = q_2(x) \implies r_1(x) = r_2(x)$.