Наибольший общий делитель многочленов. Теорема существования. Ассоциированность НОД.

НОД многочленов Пусть $f(x), g(x)$ - многочлены над F. многочлен $d(x)$ - НОД, если $f(x) = 0$ и $d(x) = 0$ или $f(x) \neq$ и $g(x) \neq 0$ и $\forall c(x) : c(x) \mid f(x) \wedge c(x) \mid g(x) \quad c(x) \mid d(x)$

Теорема существования НОД

Для любой пары $f(x), g(x) \in F[x]$, если $d(x)$ = НОД$(f(x), g(x))$ существуют многочлены $u(x)$ и $v(x)$ такие, что $f(x)u(x) + g(x)v(x) = d(x)$

Доказательство

$f(x) = r_{-1}(x)$

$g(x) = r_0(x)$

1. Случай $f(x) = g(x) = 0$. Тогда $d(x) = 0$ и $u(x), v(x)$ - любые
2. Случай $f(x) = 0, \ g(x) \neq 0$. Тогда $d(x) = g(x)$, $u(x)$ - любой, $v(x) = 1$
3. Случай $f(x) \neq 0, \ g(x) \neq 0$. Из равенств, которые возникают в алгоритме Евклида, можно получить рекуррентные формулы для $u(x)$ и $v(x)$.

   Покажем, что для любого остатка, возникающего в алгоритме Евклида, существуют многочлены $u_k(x)$ и $v_k(x)$ такие, что $r_k(x) = f(x)u_k(x) + g(x)v_k(x)$.

   По алгоритму Евклида:
   Пусть $f(x) = r_{-1}(x)$ и $g(x) = r_0(x)$

$$f(x) = 1 \cdot f(x) + 0 \cdot g(x), u_{-1}(x) = 1 \implies v_{-1}(x) = 0$$

$$g(x) = 0 \cdot f(x) + 1 \cdot g(x) \implies u_0(x) = 0, v_0(x) = 1$$

$$r_1(x) = f(x) - q_1(x)g(x)$$

$$r_1(x) = r_{-1}(x) - q_1(x)r_0(x) =$$

$$= (u_{-1}(x)f(x) + v_{-1}(x)g(x)) + q_1(x)(u_0(x)f(x) + v_0(x)g(x)) =$$

$$= (u_{-1}(x) - q_1(x)u_0(x))f(x) + (v_{-1}(x) - q_1(x)v_0(x))$$

   Если $r_{i-1}(x) = u_{i-1}(x)f(x) + v_{i-1}(x)g(x)$, а $r_i(x) = u_i(x)f(x) + v_i(x)g(x)$, то

$$r_{i+1}(x) = r_{i-1}(x) - q_i(x)r_i(x) =$$

$$= u_{i-1}(x)f(x) + v_{i-1}(x)g(x) - q_i(x)(u_i(x)f(x) + v_i(x)g(x)) =$$

$$= (u_{i-1}(x) - q_i(x)u_i(x))f(x) + (v_{i-1}(x) = q_i(x)v_i(x))v(x)$$

   Тогда $u_{i+1}(x) = u_{i-1}(x) - q_1(x)u_i(x)$ и $u_i + 1(x) = v_{i-1}(x) - q_i(x)v_i(x)$

   Таким образом, мы видим, что для всех $i \geq 1$ мы имеем разложение $r_i(x) = u_i(x)f(x) + v_i(x)g(x)$. Итак, поскольку $d(x)$ является одним из остатков в алгоритме евклида, то на каком-то шаге мы найдём разложение $d(x) = u(x)f(x) + v(x)g(x)$