Аналогично определяется наименьшее общее кратное (НОК) ненулевых многочленов $f_1(x), \dots, f_m(x)$: слово „делитель" заменяется на „кратное".

Равенство вида

$$d(x) = НОД(f_1(x), \dots, f_m(x))$$

означает, что многочлен $d(x)$ является одним из НОД многочленов $f_1(x), \dots, f_m(x)$.

Аналогично следует понимать равенство

$$m(x) = НОК(f_1(x), \dots, f_m(x))$$

Замечание

1. Из определений формально не следует, что НОД и НОК данных многочленов существуют.

   На самом деле, как будет показано ниже, они существуют.

2. Если $d(x)$ некоторый НОД многочленов $f_1(x), \dots, f_m(x)$, то любой другой НОД этих многочленов $\tilde{d}(x)$ связан с $d(x)$ соотношением:

$$\tilde{d}(x) = c \cdot d(x)$$

   где $c \in F$, $c \neq 0$.

   Аналогичное утверждение справедливо и в отношении НОК

   Говорят, что многочлены $f(x)$ и $g(x) \in F[x]$ ассоциированы, если $f(x) = c\,g(x)$, где $0 \neq c \in F$

Пусть сначала $m = 2$.

Теорема 6 (алгоритм Евклида отыскания НОД многочленов $f(x)$ и $g(x)$)

Пусть $f(x), g(x) \in F[x]$, $g(x) \neq 0$

Если $f(x)$ делится на $g(x)$, то $g(x) = НОД(f(x), g(x))$

иначе

$$f(x) = g(x)q_1(x) + r_1(x), \quad \deg r_1(x) < \deg g(x)$$

$$g(x) = r_1(x)q_2(x) + r_2(x), \quad \deg r_2(x) < \deg r_1(x)$$

$$r_1(x) = r_2(x) q_3(x) + r_3(x) \quad \deg r_3(x) < \deg r_2(x)$$

...

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

$$r_{n-1}(x) = r_n(x) q_{n+1}(x)$$

для некоторого $n \geq 1$.

Тогда $r_n(x) = НОД(f(x), g(x))$

Эта процедура последовательных делений с остатками наз алгоритмом Евклида

Доказательство

К.к $\deg g(x) > \deg r_1(x) > \deg r_2(x) > \dots$ то алгоритм Евклида конечен — завершится не более чем за $\deg g(x)$ шагов.

Если $f(x)$ делится на $g(x)$, то $g(x)$ явл. $НОД(f(x), g(x))$, т.к. соответствует определению.

Нужно теперь проверить, что $r_n(x)$ обладает всеми свойствами НОД.

Достаточно пройти по стрелкам алгоритма Евклида сначала снизу вверх, а затем сверху вниз

Теорема 7 (о линейной форме $НОД(f(x), g(x))$)

Пусть $d(x) = НОД(f(x), g(x))$, где $f(x), g(x) \in F[x]$

Тогда существуют $u(x), v(x) \in F[x]$ такие, что

$$d(x) = f(x) u(x) + g(x) v(x). \quad (**)$$

Можно считать, что

$$\deg u(x) < \deg g(x) - \deg d(x)$$
$$\deg v(x) < \deg f(x) - \deg d(x) \quad (*)$$

Замечание

Ограничения (*) дают возможность искать линейную форму НОД методом неопределенных коэффициентов.

Доказательство

Возможность линейно выразить $d(x)$ через $f(x)$ и $g(x)$ вытекает непосредственно из алгоритма Евклида.

Двигаемся по строчкам алгоритма Евклида снизу вверх.

Итак, можно считать, что рав-во (***) с некоторыми $u(x)$ и $v(x)$ получено.

1 Пусть сначала $d(x)=1$. Если, например,

$$\deg u(x) < \deg g(x)$$

то обязательно

$$\deg v(x) < \deg f(x)$$

то следует из анализа равенства

$$g(x)v(x) = 1 - f(x)u(x)$$

Если же, например,

$$\deg u(x) \geq \deg g(x)$$

то разделим $u(x)$ на $g(x)$ с остатком,

$$u(x) = g(x)\cdot q(x) + \tilde{u}(x)$$

где $\deg \tilde{u}(x) < \deg g(x)$.

Имеем:

$$1 = f(x)\big(g(x)q(x) + \tilde{u}(x)\big) + g(x)v(x) =$$
$$= f(x)\tilde{u}(x) + g(x)\tilde{v}(x)$$

где $\tilde{v}(x) = v(x) + f(x)q(x)$

Причем в этом представлении уже выполнено нужное ограничение

$$\deg \tilde{u}(x) < \deg g(x)$$

2. Общий случай.

Положим $f_1(x) = f(x)/d(x)$, $g_1(x) = g(x)/d(x)$ при этом НОД$(f_1(x), g_1(x)) = 1$.

По доказанному существуют такие $u'(x)$ и $v'(x)$, что

$$1 = f_1(x)u(x) + g(x)v(x) \quad (*)$$

$$\deg u(x) < \deg g_1(x) = \deg g(x) - \deg d(x)$$

$$\deg v(x) < \deg f_1(x) = \deg f(x) - \deg d(x)$$

Ясно, что равенство $(*)$ эквивалентно (после умножения на $d(x)$) некоторому искомому линейному представлению $d(x)$

Опр Многочлены $f_1(x), \dots, f_m(x) \in F[x]$ называются взаимно простыми, если

$$НОД(f_1(x), \dots, f_m(x)) = 1$$

Замечание

Из теорем 7 вытекает следующий критерий взаимной простоты 2 многочленов:

Многочлены $f(x), g(x)$ взаимно просты $\Leftrightarrow$ существуют такие многочлены $q(x)$ и $v(x)$, что

$$1 = f(x)u(x) + g(x)v(x)$$

Свойства взаимно простых многочленов

Пусть $f(x), g(x), h(x) \in F[x]$

1. Если $f(x)g(x)$ делится на $h(x)$ и $НОД(f(x), h(x)) = 1$, то $g(x)$ делится на $h(x)$.
2. Пусть $НОД(f(x), g(x)) = 1$. Тогда $h(x)$ делится на $f(x)g(x) \Leftrightarrow h(x)$ делится и на $f(x)$, и на $g(x)$.
3. Пусть $НОД(f(x), g(x)) = НОД(f(x), h(x)) = 1$. Тогда $НОД(f(x), g(x)h(x)) = 1$.

Доказательство (1)

Имеем по критерию взаимной простоты

$$1 = f(x)u(x) + h(x)v(x)$$

для нек-рых $u(x), v(x) \in F[x]$.

Умножим обе части на $g(x)$:

$$g(x) = \underbrace{(f(x)g(x))u(x)}_{\text{делится на } h(x)} + \underbrace{h(x)v(x)g(x)}_{\text{также очевидно делится}} \Rightarrow \text{вся сумма, т.е. } g(x) \text{ делится на } h(x)$$