Най – голям общ делител на полином

Преди да дефинираме най-голям общ делител на полиноми ще докажем следната необходима

Теорема 1:
Нека F е поле. *За всеки два полинома* $f(x),g(x) \in F[x]$, $g(x) \neq 0$ *съществуват полиноми* $q(x),r(x) \in F[x]$ *такива*, *че* $f(x) = g(x)q(x) + r(x)$, *където* ст.$r(x)$ < ст.$g(x)$ *или* $r(x) = 0$(*нулев полином*). *Полиномите* $q(x)$ *и* $r(x)$ *са единствените*, *които удовлетворяват тези условия*.
Д-во:
1. **Съществуване**
Ако $f(x)$ се дели на $g(x)$, тогава $f(x) = g(x)h(x) + 0$ и поради това съществуването на $q(x)$ и $r(x)$ е очевидно. Ето защо ще предполагаме, че

$f(x)$ не се дели на $g(x)$ (*)

Ако ст. $g(x)$ > ст. $f(x)$, тогава $f(x) = \underset{\|}{0}.\ g(x) + \underset{\|}{f(x)}$ и съществуването на $q(x)$ и $r(x)$ също е очевидно.

$q(x)$ $r(x)$

Поради това ще е предполагаме, че

ст.$g(x) \leq$ ст.$f(x)$ (**)

По-нататък доказателството ще направим по индукция относно n = ст. $f(x)$. Нека

$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, $a_n \neq 0$
$g(x) = b0 + b_1x + \ldots + b_mx^m$, $b_m \neq 0$

База n = 0 имаме $f(x) = a_0$, $a_0 \neq 0$ и $g(x) = b_0$, $b_0 \neq 0$ и очевидно

$$f(x)=\underset{\|}{(a_0b_0^{-1})}b_0 + \underset{\|}{0}$$

$q(x)$ $r(x)$

С което базата е доказана.
Нека $n \geq 1$
Разглеждаме $h(x) = f(x) - x^{n-m}.\ \frac{a_n}{b_m}.\ g(x)$
Съгласно (**) $h(x)$ е полином. Съгласно (*) $h(x)$ е ненулев полином. Тъй като $h(x)$ е разлика на два полинома от $n^{та}$ степен, в който коефициентите пред $n^{тата}$ степен са равни, имаме ст. $h(x) < n$. За $h(x)$ прилагаме индуктивната хипотеза и получаваме

$h(x) = q_1(x)\ g(x) + r_1(x)$, където ст. $r_1(x) <$ ст.$g(x)$ или $r_1(x) = 0$

от последното равенство следва

$$f(x) = h(x) + a_n\ x^{n-m}\ g(x) = q_1(x)\ g(x) + r_1(x) + \frac{a_n}{b_n} x^{n-m}\ g(x).$$

Откъдето получаваме

$$f(x) = (q_1(x) + \frac{a_n}{b_n} x^{n-m})\ g(x) + r_1(x)$$

и търсените полиноми $q(x)$ и $r(x)$ са

$q(x)= (q_1(x) + \frac{a_n}{b_n} x^{n-m})$ и $r(x)=r_1(x)$.

2.**Единственост**
Нека освен

$$f(x) = g(x)q(x) + r(x), \text{ където ст.}r(x) < \text{ст.}g(x) \text{ или } r(x) = 0$$

имаме

$$f(x) = g(x)q_1(x) + r_1(x), \text{ където ст.}r_1(x) < \text{ст.}g(x) \text{ или } r_1(x) = 0.$$

Като извадим тези две равенства получаваме

$$g(x)(q(x) – q_1(x)) = r_1(x) - r(x). \qquad (***)$$

Да допуснем, че $q(x) \neq q_1(x)$ тогава от лявата страна на последното равенство имаме ненулев полином чиято степен не е по-малка от степента на g(x). От ограниченията за r(x) и $r_1(x)$ следва, че в дясната част на това равенство стои полином, чиято степен да е по-малка от степента на g(x). Полученото противоречие доказва, че $q_1(x) = q(x)$.
Като заместим в (***) получаваме $r_1(x) - r(x) = 0$, т.е. $r_1(x) = r(x)$.
$\Rightarrow$ q(x) и r(x) са единствени□

Определение:
Нека F *е поле и* f(x) и g(x) $\in$ F[x]. *Най-голям общ делител на* f(x) *и* g(x) (НОД) *наричаме такъв полином* d(x) $\in$ F[x], *че*:

1) d(x) *дели* f(x) *и* g(x)
2) *ако* $d_1(x)$ *дели* f(x) *и* g(x), *тогава* $d_1(x)$ *дели* d(x)

Теорема 2:
Нека F *е поле. Тогава всеки два полинома от* F[x] *имат* НОД.
Д-во:
Нека f(x), g(x) $\in$ F[x].
Ако f(x) = g(x), тогава НОД е f(x).
Поради това ще предполагаме, че

$$f(x) \neq g(x) \qquad (\#)$$

Дефинираме

$$S = \{M(x) f(x) + N(x) g(x) | M(x), N(x) \in F[x]\}$$

Като положим N(x) = 0 и M(x) = 1 получаваме f(x) $\in$ S, а като положим N(x) = 1 и M(x) = 0 получаваме g(x) $\in$ S. Следователно f(x), g(x) $\in$ S. От (#) $\Rightarrow$ в S има ненулеви полиноми. Измежду всички ненулеви полиноми в S избираме такъв ненулев полином d(x), който има най-ниска възможна степен. Имаме

$$\text{ст.}d(x) \leq \text{ст. } h(x), \text{ за всеки ненулев } h(x) \in S \qquad (\#\#)$$

От d(x) $\in$ S следва

$$d(x) = M_0(x) f(x) + N_0(x) g(x) \qquad (\#\#\#)$$

Ще докажем че d(x) е най-голям общ делител на f(x) и g(x).

I. Защо d(x) е общ делител на f(x) и g(x)?

Допускаме, че d(x) не дели f(x). Тогава f(x) = d(x) q(x) + r(x), където ст.r(x) < ст.d(x). Като използваме (###) получаваме

$r(x) = f(x) - d(x)\,q(x) = f(x) - (M_0(x)\,f(x) + N_0(x)\,g(x))\,q(x) = (1 - M_0(x)\,q(x))\,f(x) - N_0(x)\,q(x)\,g(x)$

следователно, $r(x) = M(x)\,f(x) + N(x)\,g(x)$ поради това $r(x) \in S$.
Полиномът r(x) принадлежи на множеството S и има степен по-малка от d(x), което е противоречие понеже d(x) има степен най-малка в множеството S. По-същият начин се доказва, че d(x) дели g(x).
II.Нека $d_1(x)$ дели f(x) и g(x). От (###) следва, че $d_1(x)$ дели d(x).
Теоремата е доказана□

По-нататък ще ни е необходима следната

Лема:
Нека K *е комутативен пръстен, в който няма делители на нулата. Ако два ненулеви полинома от* K[x] *се делят взаимно, тогава всеки от тези полиноми може да се получи от другия чрез увножаване с ненулева константа*.
Д-во
От условието имаме
f(x) = g(x).h(x)
g(x) = f(x).t(x).

От тези две равенства получаваме f(x) = f(x).t(x). h(x). Следователно
ст.f(x) = ст.f(x) + ст.t(x) + ст.h(x). Това равенство ни дава, че ст.t(x) + ст.h(x) = 0, т.е.
ст.h(x) = ст.t(x) = 0. Доказахме Лемата тъй-като $h(x) = \text{const} \neq 0$ и $t(x) = \text{const} \neq 0$□

Следствие 1:
Нека f(x) *и* g(x) *са ненулеви полиноми. Тогава всеки* НОД *на тези полиноми може да се получи от кой да е друг* НОД *чрез умножаване с константа.*
Д-во:
Съгласно определението за НОД всеки дна най-големи общи делители на f(x) и g(x) се делят взаимно. От Лемата следва, че всеки НОД може да се получи от кой да е друг чрез умножаване с ненулева константа.

Следствие 2:

Всеки НОД d(x) *на* f(x) *и* g(x) *може да се представи във вида:*

$$d(x) = M(x)\,f(x) + N(x)\,g(x), \qquad M(x), N(x) \in F[x]$$

Д-во:
От доказателството на Теорема 2 следва, че един НОД на f(x) и g(x) може да се представи в този вид. Тъй като всеки друг НОД може да се получи от този НОД с умножаване с ненулева константа. Следствието е доказано.

Следствие 3:

Нека f(x) *и* g(x) *са от* F[x]. *Елементът* $\alpha \in F$ *е общ корен на* f(x) *и* g(x) *тогава и само тогава, когато* α *е корен на* НОД *на* f(x) *и* g(x).

Д-во:
1. Нека d(x) е НОД на f(x) и g(x) и α е корен на f(x) и g(x), т.е. $f(\alpha) = g(\alpha) = 0$
Понеже $d(x) = M(x)\,f(x) + N(x)\,g(x)$ имаме $d(\alpha) = M(\alpha)f(\alpha) + N(\alpha)g(\alpha) = 0 \Rightarrow \alpha$ е корен на d(x).

2. Нека α е корен на d(x), т.е. $d(\alpha)=0$
$f(x) = d(x)f_1(x) \Rightarrow f(\alpha) = 0$
$g(x) = d(x)g_1(x) \Rightarrow g(\alpha) = 0$
следователно α е общ корен на f(x) и g(x).□
По нататък НОД на f(x) и g(x) макар да не е определен еднозначно ще го означаваме с (f(x), g(x))

Алгоритъм на Евклид за намиране на НОД

Нека F е поле и $f(x)$ и $g(x) \in F[x]$. Прилагайки последователно Теорема 1 получаваме равенствата:

$f(x) = g(x)q_1(x) + r_1(x)$, където ст.$r_1(x)$ < ст.$g(x)$
$g(x) = r_1(x)q_2(x) + r_2(x)$, където ст.$r_2(x)$ < ст.$r_1(x)$
$r_1(x) = r_2(x)q_3(x) + r_3(x)$, където ст.$r_3(x)$ < ст.$r_2(x)$
$r_2(x) = r_3(x)q_4(x) + r_4(x)$, където ст.$r_4(x)$ < ст.$r_3(x)$
:
$r_k(x) = r_{k+1}(x)q_{k+2}(x) + r_{k+2}(x)$, където ст.$r_{k+2}(x)$ < ст.$r_{k+1}(x)$
$r_{k+1}(x) = r_{k+2}(x)q_{k+3}(x) + 0$
$r_{k+2}(x)$ – последният ненулев остатък

Твърдение:

$r_{к+2}(x)$ е НОД *на* f(x) *и* g(x)

Д-во:
Движейки се по равенствата отдолу нагоре получаваме, че $r_{к+2}(x)$ е общ делител на f(x) и g(x). Ако d(x) дели f(x) и g(x) чрез движение по равенствата отгоре надолу доказваме, че d(x) дели $r_1(x), r_2(x), \ldots, r_{k+2}(x) \in S$. □