Делимост на полиноми над поле

Нека $f, g \in F[x]$, F – поле.

D Казваме, че полином g дели f и означаваме $g \mid f$, ако $\exists h \in F[x] : f = g.h$

В противен случай: $g \nmid f$

Свойства:

1) $af \mid bf$, $a \neq 0$, $a, b \in F$, $f \neq 0$
2) $g \mid f \Rightarrow ag \mid bf$, $a \in F^*$, $b \in F$
3) $f \mid g$, $g \mid f \Rightarrow f = ag$, $a \in F^*$
4) $f \mid g$, $g \mid h \Rightarrow f \mid h$
5) $f \mid g_i$, $i = \overline{1,k} \Rightarrow f \mid g_1 h_1 + \ldots + g_k h_k$, $h_i \in F[x]$.
6) $f \mid g_1 + g_2$, $f \mid g_1 \Rightarrow f \mid g_2$

D $f, g \in F[x]$, $g \neq 0$. Казваме, че $d \in F[x]$ е НОД на f и g и означаваме $(f, g) = d$, ако:

1) $d \mid f$, $d \mid g$
2) $d_1 \mid f$, $d_1 \mid g \Rightarrow d_1 \mid d$

Забележка: НОД ще бъде определен с точност до константа $\Rightarrow$ $\Rightarrow$ за единственост взимаме унитарния полином,

$(f, g) = d \Rightarrow (f, g) = ad$, $a \neq 0$, $a = const$

Тв Нека $f, g \in F[x]$, F – поле, $g \neq 0$. Тогава $\exists d \in F[x] : (f, g) = d$

Д Док-во: $F[x] \to I = (f, g) = \{uf + vg \mid u, v \in F[x]\} \trianglelefteq F[x]$

По твърдение $\Rightarrow I = (d) \trianglelefteq F[x]$. Ще покажем, че $(f, g) = d$.

$d = uf + vg$ (Тождество на Безу)

1) $d \mid f$; $d \mid g$?

$f \in I = (d) \Rightarrow f = df_1 \Rightarrow d \mid f$

$g \in I = (d) \Rightarrow g = dg_1 \Rightarrow d \mid g$

$\Big\} (f, g) = d$

2) $d_1 \mid f$, $d_1 \mid g \Rightarrow d_1 \mid \underbrace{uf + vg}_{d} \Rightarrow d_1 \mid d$

II) Док-во: (Алгоритъм на Евклид)

$f, g \in F[x]$, $g \neq 0$.

$f = gq + r$, $\deg r < \deg g$

Ако $r = 0 \Rightarrow g \mid f \Rightarrow (f,g) = g$

Ако $r \neq 0$:

$g = rq_1 + r_1$ $\deg r_1 < \deg r$

Ако $r_1 = 0 \Rightarrow (f,g) = r$

....

$r_{i-1} = r_i q_{i+1} + r_{i+1}$

$= 0 \Rightarrow r_i = ad$, $d = (f,g)$

1) r_i стъпка по стъпка се доказва, че дели всяко нагоре

2) $d_1 \mid f$, $d_1 \mid g \Rightarrow d_1 \mid r \Rightarrow d_1 \mid r_1 \dots d_1 \mid r_i$

$\Rightarrow f(\dots) \cdot u + g(\dots) \cdot v = ad$

D $f_1 \dots f_k \in F[x]$

$(f_1 \dots f_k) := ((f_1 \dots f_{k-1}), f_k)$

D $(f,g) = c \Rightarrow (f,g) = 1$ – взаимно прости

$\Leftrightarrow c \in F^*$

Забележка: $(f,g) = 1 \Leftrightarrow \exists!\, u, v \in F[x] : uf + vg = 1$

Тв $u \mid fg$ и $(u,f) = 1 \Rightarrow u \mid g$

Тв $g_1 \mid f$, $g_2 \mid f$, $(g_1, g_2) = 1$

D НОК: $f, g \neq 0$, $f, g \in F[x]$.

Казва се, че $m = [f,g]$ е НОК на f и g, ако:

1) $f \mid m$ и $g \mid m$

2) $f \mid m_1$ и $g \mid m_1 \Rightarrow m \mid m_1$

Тв $f, g \in F$, $f \neq 0 \neq g \Rightarrow (fg)[f,g] = afg$, $a \in F^*$

D Нека F – поле, $f \in F[x]$, $\deg f \geq 1$. f се нарича неразложим над F, ако не може да се представи като произведение на два полинома от по-ниска степен. В противен случай се нарича разложим

Δ
$\Leftrightarrow$
∇

Ако $f = gh \Rightarrow \deg g = \deg f$ или $\deg h = \deg f$

$\Rightarrow$ Св-во: Ако f е неразложим, то делителите на f са αf или α, $\alpha \in F^*$.

Нека g – неразложим полином над F. $(g,h) = \begin{cases} \text{const} & g \nmid h \\ g & g \mid h \end{cases}$

T F – поле. Всеки полином от степен ≥ 1 може да се представи като произведение на неразложими полиноми. Това представяне е единствено с точност до константа и с точност до реда на множителите.

$f = g_1 \dots g_t = h_1 \dots h_s \Rightarrow t = s$, $\exists$ пермутация $h_1' \dots h_s'$: $\alpha_i h_i' = g_i$ и $\alpha_1 \dots \alpha_s = 1$.

g_i, h_j – неразложими

Доказателство: индукция по степента на f (за $\exists$)

Полиномите от първа степен са неразложими

1) $\deg f = 1 \Rightarrow f$ – неразложим

2) Нека е в сила за всеки полином от степен, по-малка от $n = \deg f$.

3) 1. Ако f – неразложим $\Rightarrow$ ✓

2. Ако f – разложим $\Rightarrow \exists g, h : f = gh$ и $\deg g < \deg f$, $\deg h < \deg f$

$\rightarrow$ прилагаме индукцията за g и h:

$\exists g_1 \dots g_s = g$, $h_1 \dots h_t = h$: g_i, h_j – неразложими

$\Rightarrow f = g_1 \dots g_s h_1 \dots h_t$ – представяне на f като произведение на неразложими множители

!) Нека $f = g_1 \dots g_t = h_1 \dots h_s$, g_i, h_j – неразложими

$g_1 \dots g_t = h_1 \dots h_s$

$g_1 \mid h_1 \dots h_s \Rightarrow (g_1, h_i) = \begin{cases} 1 & g_1 \nmid h_i \\ g_1 & g_1 \mid h_i \end{cases}$

Ако допуснем, че $(g_1, h_i) = 1$, $\forall i \Rightarrow g_1 \nmid h_1 \dots h_s \Rightarrow \exists h_j : g_1 \mid h_j$

Преназначаване: [illegible]

$h_j = h_1' \Rightarrow g_1 \mid h_1' \Rightarrow h_1' = \alpha_1 g_1$, $\alpha_1 \in F^*$

... // Аналогично правим и другите

$\Rightarrow g_1 \dots g_t = h_1' \dots h_s' \Rightarrow g_2 \dots g_t = h_2' \dots h_s'$

Не е възможно s и t да са различни, защото от едната страна бихме останали полиноми, а от другата – константи $\Rightarrow s = t$

$\Rightarrow g_i = \alpha_i h_i' \Rightarrow 1 = \alpha_1^* \dots \alpha_t$

Разлагане на полиноми над $\mathbb{Z}$ и $\mathbb{Q}$

$f(x) \in \mathbb{Q}[x]$

$f = a_0 + a_1 x + \dots + a_s x^s$

$a_i = b_i / c_i$, $b_i, c_i \in \mathbb{Z}$

$НОК(c_0 \dots c_s) = c \in \mathbb{Z}$

$$f = \frac{1}{c}\left(\underbrace{\frac{b_0}{c_0}}_{l_0} \cdot c + \underbrace{\frac{b_1}{c_1}}_{l_1} c x + \dots + \underbrace{\frac{b_s}{c_s}}_{l_s} c x^s\right) \longrightarrow l_i \in \mathbb{Z}$$

$НОД(l_0 \dots l_s) = l$

$$f = \frac{l}{c}\left(\underbrace{\frac{l_0}{l}}_{h_0} + \underbrace{\frac{l_1}{l}}_{h_1} x + \dots + \underbrace{\frac{l_s}{l}}_{h_s} x^s\right) \Rightarrow h_i \in \mathbb{Z}$$

$$f = \frac{l}{c}\left(h_0 + h_1 x + \dots + h_s x^s\right), \quad НОД(h_0 \dots h_s) = 1$$

D $\hookrightarrow$ примитивен полином – полином с $\mathbb{Z}$ коефициенти $h_0 \dots h_s : НОД(h_0 \dots h_s) = 1$

Св-во: Всеки полином над $\mathbb{Q}$ може да се представи като рационална константа, умножена с примитивен полином.

($\forall f \in \mathbb{Q}[x] \Rightarrow f = \alpha g$, $\alpha \in \mathbb{Q}$, $g \in \mathbb{Z}[x]$)

Л Лема на Гаус

Произведението на два примитивни полинома с цели коефициенти е примитивен полином