10.05.2016

(16) Разлагане на полиноми с цели и с рационални коефициенти - лема на Гаус и критерий на Айзенщайн.

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

$f = a_0 + a_1 x + \dots + a_s x^s$, $a_i = \frac{b_i}{c_i}$, $b_i, c_i \in \mathbb{Z}$

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

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

$НОД(l_0, \dots, l_s) = l$

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

$f = \frac{l}{c}(h_0 + h_1 x + \dots + h_s x^s)$, $h_i \in \mathbb{Z}$,

$НОД(h_0, \dots, h_s) = 1$

Деф: Примитивен полином е такъв полином над $\mathbb{Z}$, който има цели коефициенти, за които НОД на всички коефициенти на полинома е 1.

Свойство: Всеки полином ~~над $\mathbb{Q}$~~ $f \in \mathbb{Q}[x]$ може да се представи във вида $f = \alpha \cdot g(x)$, където $\alpha \in \mathbb{Q}$,

$g(x) \in \mathbb{Z}[x]$ и g е примитивен.

Лема (на Гаус)

Произведението на два примитивни полинома с цели коефициенти е примитивен полином.

Доказателство:

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

$f(x) = a_0 + a_1 x + \ldots + a_s x^s$

$n \in \mathbb{Z}$

$\varphi: \mathbb{Z}[x] \to \mathbb{Z}_n[x]$

$\varphi(f) = \bar{a}_0 + \bar{a}_1 x + \ldots + \bar{a}_s x^s$, $\bar{a}_i \in \mathbb{Z}_n$

$\varphi(f+g) = \varphi(f) + \varphi(g)$

$\varphi(fg) = \varphi(f) \cdot \varphi(g)$

→ Нека f, g - примитивни, $h = f \cdot g$

Допускаме, че h не е примитивен, т.е. $\exists p$ - просто ; което дели всички коефициенти на h

$\varphi: \mathbb{Z}[x] \to \mathbb{Z}_p[x]$

$\varphi(f \cdot g) = \varphi(h) = 0$

f - примитивен $\Rightarrow \exists k: p \nmid f_k$

$f = f_0 + f_1 x + \ldots + f_\ell x^\ell$

g - примитивен $\Rightarrow \exists t: p \nmid g_t$

$g = g_0 + g_1 x + \ldots + g_m x^m$

$\varphi(h) = 0 = \varphi(g) \cdot \varphi(f)$

$\varphi(g) \neq 0$ ($\bar{g_t} \neq 0$); $\varphi(f) \neq 0$ ($\bar{f_k} \neq 0$) — остатък

$0 = \underbrace{\varphi(f)} \cdot \underbrace{\varphi(g)}$ ↯ с допускането, че h не е примитивен

$0 = \bar{f} \cdot \bar{g}$ ($\mathbb{Z}_p$ е поле)

$\Rightarrow h$ е примитивен полином

Th Нека h - примитивен полином, $\alpha \in \mathbb{Q}$: $\alpha h \in \mathbb{Z}[x]$. Тогава $\alpha \in \mathbb{Z}$

Доказателство: $\alpha = \frac{a}{b}$, $a, b \in \mathbb{Z}$, $(a, b) = 1$

$\alpha h = \alpha(h_0 + h_1 x + \ldots + h_s x^s) \in \mathbb{Z}$, $\alpha h_i \in \mathbb{Z}$

$\alpha h_i \in \mathbb{Z} \Rightarrow \frac{a h_i}{b} \in \mathbb{Z} \Rightarrow b \mid h_i$, $i = 0, \ldots, s$

$\Rightarrow b \mid \text{НОД}(h_0, \ldots, h_s) = 1 \Rightarrow b \mid 1 \Rightarrow \alpha = \frac{a}{b} \in \mathbb{Z}$,

$b = \pm 1$

Th. Нека $f(x) \in \mathbb{Z}[x]$, $\deg f \geq 1$, f е неразложим над $\mathbb{Z} \Leftrightarrow f$ е неразложим над $\mathbb{R}$

Доказателство:

$\Rightarrow$ Нека f е неразложим над $\mathbb{Z}$ и допускаме, че е разложим над $\mathbb{R}$.

$f = h \cdot g$: $h, g \in \mathbb{Q}[x]$, $\deg h < \deg f$, $\deg g < \deg f$.

$h = \alpha \cdot h_1(x)$, $h_1 \in \mathbb{Z}[x]$, h_1 - примитивен

$g = \beta g_1(x)$, $g_1 \in \mathbb{Z}[x]$, g_1 - примитивен, $\alpha, \beta \in \mathbb{Q}$

$f = \alpha . \beta . \underbrace{h_1 . g_1}$
примитивно

$\left.\begin{array}{l} f \in \mathbb{Z}[x] \\ \alpha\beta \in \mathbb{Q} \\ h_1 g_1 \text{ - примитивни} \end{array}\right\} \Rightarrow \alpha\beta \in \mathbb{Z}$

$f = \underbrace{(\alpha\beta h_1)}_{\in \mathbb{Z}[x]} g_1 \in \mathbb{Z}[x]$ $\Rightarrow$

$\Rightarrow$ разлагане на полинома f над $\mathbb{Z}$ $\Rightarrow$ (4) $\Rightarrow$

$\Rightarrow$ f е неразложим над $\mathbb{Q}$

$\Leftarrow$ Директно следва

Th. (Критерий на Айзенщайн)

Нека $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n \in \mathbb{Z}[x]$

Ако $\exists$ p - просто:

1) $p \nmid a_0$;

2) $p \mid a_1, p \mid a_2, \ldots, p \mid a_n$;

3) $p^2 \nmid a_n$;

Тогава $f(x)$ е неразложим над $\mathbb{Q}$ (над $\mathbb{Z}$).

Доказателство:

Допускаме, че $f(x)$ - разложим над $\mathbb{Z}$

$f(x) = g(x) . h(x)$, $\deg g < n$, $\deg h < n$, $g(x), h(x) \in \mathbb{Z}[x]$

$\varphi: \mathbb{Z}[x] \to \mathbb{Z}_p[x]$

$\varphi(f) = \bar{a}_0 x^n = \varphi(g) \cdot \varphi(h)$

$\mathbb{Z}_p$ - поле $\quad \varphi(f(x)) = \bar{a}_0 x \cdot x \cdot x \cdot \ldots \cdot x$

$\Rightarrow \varphi(g), \varphi(h)$ имеют только неразложимые множители dx

$\varphi(g) = \alpha_1 x^s$

$\varphi(h) = \beta_1 x^t$, $s + t = n$

$g = g_0 + g_1 x + \ldots + g_s x^s$

$\Rightarrow g_0 = \bar{g}_1 = \ldots = \bar{g}_{s-1} = \bar{0}$

$\Rightarrow p \mid g_0, p \mid g_1, \ldots, p \mid g_{s-1}$

$h = h_0 + h_1 x + \ldots + h_t x^t$

$p \mid h_0, \ldots, p \mid h_{t-1}$

$f = a_0 x^n + \ldots + a_n$

$a_n = g_0 h_0 \Rightarrow p^2 \mid a_n$

$p \mid g_0, p \mid h_0$

$p^2 \mid a_n \Rightarrow$ (4)

$\Rightarrow f$ - неразложим

Пример: $x^{2016} + 2$

Следствие: Над полето на целите числа има неразложими полиноми от произволна степен.