Полиноми с рационални коефициенти. Критерии за неразложимост.

Разглеждаме неконстантният полином $f(x) \in \mathbb{Q}[x]$. Интересува ни въпросът дали той е разложим над $\mathbb{Q}$. Можем да запишем f като

$$f(x) = \frac{1}{a} \cdot g(x)$$

за полином $g(x) \in \mathbb{Z}[x]$, ако например числото a е равно на произведението на знаменателите на всеки от коефициентите на $f(x)$. Очевидно f и g са едновременно разложими или неразложими над $\mathbb{Q}$ и по този начин свеждаме въпроса до това дали даден полином с цели коефициенти е разложим над $\mathbb{Q}$.

Нека $g(x) = b_0x^n + b_1x^{n-1} + \cdots + b_{n-1}x + b_n \in \mathbb{Z}[x]$. Казваме, че $g(x)$ е *примитивен*, ако НОД на $b_0, b_1, \ldots, b_n$ е равен на 1 (или иначе казано $b_0, b_1, \ldots, b_n$ не се делят едновременно на друго цяло число освен ± 1). В общия случай, ако $(b_0, b_1, \ldots, b_n) = b \in \mathbb{Z}$, то $g(x) = bh(x)$ за полином $h(x) \in \mathbb{Z}[x]$, който е примитивен.

Нека $g(x) \in \mathbb{Z}[x]$ и p е просто число. Разглеждаме полето от остатъци

$$\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}.$$

Означаваме $\overline{g}(x) = \overline{b_0}x^n + \overline{b_1}x^{n-1} + \cdots + \overline{b_{n-1}}x + \overline{b_n}$. Полиномът $\overline{g}(x) \in \mathbb{Z}_p[x]$ се нарича *редукция на g по модул p*. Ако $p \nmid b_0$, то $\overline{b_0} \neq 0$ и $\deg \overline{g} = \deg g$. Ясно е, че g е примитивен $\iff$ за всяко просто число редукцията $\overline{g} \neq \overline{0}$.

Пример:Редукцията на полинома

$$g(x) = 4x^4 + 5x^2 + 6x + 8 \in \mathbb{Z}[x]$$

по модул 3 е

$$\overline{g}(x) = x^4 + \overline{2}x^2 + \overline{2} \in \mathbb{Z}_3[x].$$

От дефиницията на операцията $\cdot$ в полето $\mathbb{Z}_p$ за произволно просто число p следва свойството, че ако $g_1(x), g_2(x) \in \mathbb{Z}[x]$, то $\overline{g_1.g_2}(x) = \overline{g_1}(x).\overline{g_2}(x)$.

Лема на Гаус. *Ако $h_1(x), h_2(x) \in \mathbb{Z}[x]$ са примитивни полиноми, то $h_1(x)h_2(x)$ също е примитивен полином.*

Доказателство. Нека допуснем, че полиномът $h(x) = h_1(x)h_2(x)$ не е примитивен. Тогава съществува просто число p, такова че редукцията $\overline{h}(x) \in \mathbb{Z}_p[x]$ е тъждествено нулевият полином $\overline{h}(x) = \overline{0}$. Но така имаме $\overline{h}(x) = \overline{h_1(x)h_2(x)} = \overline{h}_1(x)\overline{h}_2(x) = \overline{0}$. Т.к. $\mathbb{Z}_p$ е поле, пръстенът $\mathbb{Z}_p[x]$ е област, т.е. в него няма делители на нулата и тогава $\overline{h}_1(x) = \overline{0}$ и/или $\overline{h}_2(x) = \overline{0}$. При това положение достигаме до противоречието, че $h_1(x)$ и/или $h_2(x)$ не е примитивен. Следователно остава да е вярно, че $h(x)$, т.е. $h_1(x)h_2(x)$ е примитивен. □

Забележка:
Ако $h(x) \in \mathbb{Z}[x]$ е примитивен полином, а $c \in \mathbb{Q}$ е такова число, че $ch(x) \in \mathbb{Z}[x]$, то $c \in \mathbb{Z}$.

Наистина, нека

$$h(x) = c_0x^n + c_1x^{n-1} + \cdots + c_n, \quad c_i \in \mathbb{Z}$$

и $c = \dfrac{r}{s} \in \mathbb{Q}$, където $r, s \in \mathbb{Z}$ са такива числа, че $(r, s) = 1$ (т.е. c е записано като несъкратима дроб). Сега коефициентите на $ch(x)$ са $cc_i = \dfrac{rc_i}{s} \in \mathbb{Z}$. Това означава, че $s \mid rc_i$, но $(s, r) = 1$ и следователно $s \mid c_i$ за $\forall i = 0, 1, \ldots, n$. Т.к. h е примитивен, то $(a_0, a_1, \ldots, a_n) = 1$, което означава, че $s = \pm 1$, а оттук $c = \dfrac{r}{s} = \pm s \in \mathbb{Z}$.

Следствие 1. *Полином $g(x) \in \mathbb{Z}[x]$ е неразложим над $\mathbb{Q}$ $\iff$ $g(x)$ е неразложим над $\mathbb{Z}$.*

Доказателство. Обратната посока е очевидна, т.к. $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$. Ще докажем необходимостта. Нека $g(x) \in \mathbb{Z}[x]$ е разложим над $\mathbb{Q}$, т.е. $g(x) = g_1(x)g_2(x)$ за $g_1, g_2 \in \mathbb{Q}[x]$. Представяме $g_1(x) = \dfrac{a_1}{b_1} \cdot h_1(x)$, където $a_1, b_1 \in$

$\mathbb{Z}$ и примитивен полином $h_1(x) \in \mathbb{Z}[x]$. По аналогичен начин представяме и $g_2(x) = \dfrac{b_2}{a_2} h_1(x)$. Така получаваме, че

$$g(x) = \frac{b_1 b_2}{a_1 a_2} h_1(x) h_2(x) \in \mathbb{Z}[x]$$

за $\dfrac{b_1 b_2}{a_1 a_2} = c \in \mathbb{Q}$ и примитивен полином $h_1(x)h_2(x)$ (съгласно лемата). Сега от Забележката имме, че $c \in \mathbb{Z}$ и $g(x) = \underbrace{c h_1(x)}_{\in \mathbb{Z}[x]} \underbrace{h_2(x)}_{\in \mathbb{Z}[x]}$, т.е. $g(x)$ е разложим и над $\mathbb{Z}$. $\square$

Ще разгледаме няколко критерия, които представляват достатъчно условие за разложимост на даден полином.

1. Редукционен критерий: нека $f(x) \in \mathbb{Z}[x]$ има $\deg f = n \geq 1$ и старши коефициент a_0. Ако p е просто число, което не дели a_0 и редукционният полином $\overline{f}(x) \in \mathbb{Z}_p[x]$ е неразложим над $\mathbb{Z}_p$, то $f(x)$ е неразложим над $\mathbb{Q}$.

Доказателство: допускаме противното, а именно че $f(x)$ е разложим над $\mathbb{Q}$. В такъв случай $f(x)$ е разложим и над $\mathbb{Z}$ и $f(x) = g(x)h(x)$ за полиноми $g(x), h(x) \in \mathbb{Z}[x]$ с $\deg g, \deg f \geq 1$. Имаме, че $p \nmid a_0$ и тогава $\overline{a}_0 \neq \overline{0}$ в $\mathbb{Z}_p$, а оттам и $\deg \overline{f} = \deg f = n$. Освен това $\overline{f}(x) = \overline{g(x)h(x)} = \overline{g}(x)\overline{h}(x)$ с $\deg \overline{g} = \deg g \geq 1$ и $\deg \overline{h} = \deg h \geq 1$, което е противоречие с неразложимостта на редукцията на полинома.

2. Критерий на Айзенщайн: нека $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{Z}[x]$, а p е просто число и

1) $p \nmid a_0$;

2) p дели всички останали коефициенти $a_1, a_2, \ldots, a_n$;

3) $p^2 \nmid a_n$.

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

Доказателство: отново допускаме противното. Тогава $f(x) = g(x)h(x)$ за полиноми $g, h \in \mathbb{Z}[x]$ с $\deg g = k \geq 1$ и $\deg h = l \geq 1$, $k+l = n = \deg f$. В пръстенът $\mathbb{Z}_p[x]$ за редукцията $\overline{f}(x)$ имаме $\overline{a}_0 \neq \overline{0}$ и $\overline{a}_1 = \overline{a}_2 = \cdots = \overline{a}_n = \overline{0}$. Тогава $\overline{f}(x) = \overline{a}_0 x^n$. Сега от $\overline{f} = \overline{g} \cdot \overline{h}$ следва, че $\overline{g}(x) = \overline{b}x^k$, а $\overline{g}(x) = \overline{c}x^l$, като $\overline{b}, \overline{c} \neq \overline{0}$. Ако $g(x) = bx^k + b_1 x^{k-1} + \cdots + b_k$, то тогава $b_1, \ldots, b_k$ всички се делят на p. Аналогично, ако $h(x) = cx^l + c_1 x^{l-1} + \cdots + c_l$, то p дели

$c_1, \ldots, c_l$. Така $a_n = b_k c_l$, а b_k и c_l се делят на p. Тогава $p^2 \mid a_n$, което противоречи на условие 3). Следователно $f(x)$ е неразложим над $\mathbb{Q}$.

Пример: За полинома

$$f(x) = 2x^5 - 21x^3 + 42x + 63$$

имаме при $p = 7$

$$1) 7 \nmid 2$$
$$2) 7 \mid 21, 42, 63$$
$$3) 49 \nmid 63.$$

Така $f(x)$ е неразложим над $\mathbb{Q}$. (Достатъчно е да намерим само едно просто число, за което критерият на Айзенщайн е изпълнен и f ще бъде неразложим.)

Следствие 2. *За всяко естествено число n съществува полином $f(x) \in \mathbb{Q}[x]$ от степен n, който е неразложим над $\mathbb{Q}$.*

Доказателство. За произволн число $n \in \mathbb{N}$ разглеждаме полинома

$$f(x) = x^n + 2.$$

Имаме, че $2 \nmid 1$; $2 \mid 0, 0, \ldots, 0, 2$ и $2^2 \nmid 2$, което означава, че $f(x)$ е неразложим над $\mathbb{Q}$ според критерия на Айзенщайн. $\square$