ЛЕКЦИЯ 18

ПОЛИНОМИ С РАЦИОНАЛНИ КОЕФИЦИЕНТИ. КРИТЕРИЙ НА АЙЗЕНЩАЙН.

Ако целите числа m и n са взаимно прости, ще пишем $(m, n) = 1$.
Ще ни са необходими следните елементарни твърдения от теория на числата:

Твърдение 1. *Нека m, a, $b \in \mathbb{Z}$ и m дели $a.b$. Ако $(m, a) = 1$, тогава m дели b.*

Твърдение 2. *Нека p и a са цели числа и p е просто число. Ако p не дели a, тогава $(p, a) = 1$.*

Твърдение 3. *Нека p, a_1, a_2, $\ldots$, a_k са цели числа, p е просто число и дели произведението $a_1 a_2 \ldots a_k$. Тогава p дели някое от числата a_1, a_2, $\ldots$, a_k.*

Определение. *Нека $f(x)$ е полином с цели коефициенти, т. е. $f(x) \in \mathbb{Z}[x]$. Казваме, че $f(x)$ е примитивен полином, ако единствените цели числа, които делят всичките му коефициенти, са 1 и -1.*

Твърдение 4. *Нека $f(x)$ е полином с рационални коефициенти. Тогава $f(x)$ може да се представи във вида*

$$f(x) = r.f_1(x),$$

където $r \in \mathbb{Q}$ и $f_1(x)$ е примитивен полином.

Доказателство:

Нека $f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_n}{b_n}x^n$, където a_i, b_i са цели числа.

Ако общият знаменател на $\frac{a_0}{b_0}$, $\frac{a_1}{b_1}$, $\ldots$, $\frac{a_n}{b_n}$ е равен на m, тогава имаме

$$f(x) = \frac{1}{m}(c_0 + c_1x + \cdots + c_nx^n),$$

където c_i са цели числа. Нека НОД на c_0, c_1, $\ldots$, c_n е d и $c_i = c_i'd$, $i = 0$, 1, $\ldots$, n. Тогава

$$f(x) = \frac{d}{m}(c_0' + c_1'x + \cdots + c_n'x^n),$$

където НОД на c_i', $i = 0$, 1, $\ldots$, n е равен на 1. Това означава, че $c_0' + c_1'x + \cdots + c_n'x^n$ е примитивен полином.

Лема 1. *Нека $f(x)$ е примитивен полином. Ако $r \in \mathbb{Q}$ и коефициентите на $r.f(x)$ са цели числа, тогава r също е цяло число.*

Доказателство:

Нека $f(x) = a_0 + a_1x + \cdots + a_nx^n$ и $r = \frac{b}{c}$, където b и c са цели и взаимно прости. Получаваме

$$r.f(x) = \frac{b}{c}a_0 + \frac{b}{c}a_1x + \cdots + \frac{b}{c}a_nx^n.$$

От условието имаме, че $\frac{a_ib}{c}$ е цяло число за $i = 0$, $\ldots$, n. Следователно c дели a_ib. Понеже $(c, b) = 1$ от Твърдение 1 получаваме, че c дели a_i за $i = 0$, $\ldots$, n. Числото c дели всички коефициенти на $f(x)$ и тъй като по условие $f(x)$ е примитивен имаме, че $c = \pm 1$. Следователно $r = \frac{b}{c}$ е цяло.

Лема на Гаус. *Произведението на няколко примитивни полиноми също е примитивен полином.*

Доказателство:

Достатъчно е да докажем лемата за произведението на два примитивни полинома.

Нека са дадени примитивните полиноми

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$
$$g(x) = b_0 + b_1x + \cdots + b_mx^m.$$

Разглеждаме тяхното произведение

$$h(x) = f(x)g(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}.$$

Трябва да докажем че $h(x)$ също е примитивен. Да допуснем противното, т. е. $h(x)$ не е примитивен полином. Тогава съществува просто число p, което дели всичките коефициенти на $h(x)$, т. е. p дели c_0, c_1, ..., c_{n+m}. Понеже $f(x)$ е примитивен полином имаме, че p не дели всички коефициенти на $f(x)$. Нека i е най-малкия индекс, за който p не дели a_i, т. е. p дели a_0, a_1, ..., a_{i-1} и p не дели a_i. Понеже $g(x)$ също е примитивен полином следва, че p не дели всички коефициенти на $g(x)$. Нека j е най-малкия индекс, за който b_j не се дели на p, т. е. p дели b_0, b_1, ..., b_{j-1} и p не дели b_j. Разглеждаме:

$$c_{i+j} = \underbrace{a_0b_{i+j} + a_1b_{i+j-1} + \cdots + a_{i-1}b_{j+1}}_{\text{дели се на } p} + a_ib_j + \underbrace{a_{i+1}b_{j-1} + \cdots + a_{i+j}b_0}_{\text{дели се на } p}$$

Понеже p дели c_{i+j}, следва че p трябва да дели a_ib_j. От Твърдение 3 имаме, че p дели или a_i, или b_j, което противоречи на избора на индексите i и j. С това Лемата е доказана.

Следствие. *Нека $f(x)$ е полином с цели коефициенти и $f(x)$ е разложим над $\mathbb{Q}$. Тогава $f(x)$ е разложим над $\mathbb{Z}$.*

Доказателство:

Нека $f(x) = f_1(x).f_2(x)$, където $f_1(x)$, $f_2(x) \in \mathbb{Q}[x]$ и ст. $f_1(x) \geq 1$, ст. $f_2(x) \geq 1$.

Съгласно Твърдение 4

$$f_1(x) = r_1\widetilde{f_1}(x), \text{ където } r_1 \in \mathbb{Q} \text{ и } \widetilde{f_1}(x) \text{ е примитивен}$$
$$f_2(x) = r_2\widetilde{f_2}(x), \text{ където } r_2 \in \mathbb{Q} \text{ и } \widetilde{f_2}(x) \text{ е примитивен.}$$

Тогава $f(x) = f_1(x).f_2(x) = r_1.r_2.\widetilde{f_1}(x).\widetilde{f_2}(x)$. От лемата на Гаус имаме, че $\widetilde{f_1}(x).\widetilde{f_2}(x)$ е примитивен. Понеже $f(x)$ има цели коефициенти, от Лема 1 следва $r_1.r_2 \in \mathbb{Z}$. Нека $m = r_1.r_2 \in \mathbb{Z}$. Тогава $f(x) = (m\widetilde{f_1}(x))\widetilde{f_2}(x)$ дава желаното разлагане над $\mathbb{Z}$.

Критерий на Айзенщайн за неразложимост над $\mathbb{Q}$. *Нека $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, $a_n \neq 0$, $n \geq 1$, за който съществува просто число p със следните свойства:*

1) p не дели a_n;

2) p дели останалите коефициенти a_0, ..., a_{n-1};

3) p^2 не дели a_0.

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

Доказателство:

Да допуснем противното, т. е., че $f(x)$ е разложим над $\mathbb{Q}$. Съгласно Следствието $f(x)$ е разложим и над $\mathbb{Z}$, т. е. $f(x) = g(x).h(x)$, където $g(x) \in \mathbb{Z}[x]$, $h(x) \in \mathbb{Z}[x]$ и ст. $g(x) \geq 1$, ст. $h(x) \geq 1$. Нека подробно записани тези полиноми са:

$$g(x) = b_0 + b_1x + \cdots + b_sx^s, \quad s \geq 1$$
$$h(x) = c_0 + c_1x + \cdots + c_kx^k, \quad k \geq 1$$

Имаме $a_0 = b_0.c_0$.

По условие p дели a_0. Понеже p е просто от Твърдение 3 имаме, че p дели c_0 или b_0. Без ограничение на общността можем да предположим,че p дели b_0.

От това, че a_0 не се дели на p^2 получаваме, че p не дели c_0. Съгласно Твърдение 2 имаме $(p, c_0) = 1$. Разглеждаме

$$a_1 = b_0c_1 + b_1c_0 \qquad (*)$$

По условие p дели a_1. Вече изяснихме, че p дели b_0. Поради това от (*) получаваме, че p дели b_1c_0. Понеже $(p, c_0) = 1$ от Твърдение 1 следва, че p дели b_1. От равенството

$$a_2 = b_2c_0 + b_1c_1 + b_0c_2,$$

като вземем под внимание, че a_2, b_1, b_0 се делят на p получаваме, че p дели b_2c_0. Понеже $(p, c_0) = 1$ от Твърдение 1 следва, че p дели b_2 и т. н. Понеже $s < n$, всеки от коефициентите $a_0, a_1, \ldots, a_s$ се дели на p. Поради това последователно изясняваме, че p дели $b_0, b_1, b_2, \ldots, b_s$. Разглеждаме равенството

$$a_n = a_{s+k} = b_s.c_k.$$

От това равенство следва, че p дели $a_{s+k} = a_n$, което противоречи на условието. С това противоречие теоремата е доказана.

Следствие. *За всяко естествено число n, съществува неразложим над $\mathbb{Q}$ полином от степен n.*

Такъв е например полиномът $x^n + 2$.