Fermā Lielā teorēma polinomiem

Emīls Kalugins

2020. gada 15. februārī

Fermā Lielā teorēma

Neeksistē naturāli skaitļi a, b, c, kas apmierinātu vienādību

$$a^n + b^n = c^n,$$

ja $n > 2$ ir naturāls skaitlis.

Aritmētikas pamatteorēma

Katrs naturāls skaitlis $n > 1$ ir viennozīmīgi izsakāms kā pirmskaitļu reizinājums formā

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m},$$

kur p_i ir pirmskaitļi un $\alpha_i \in \mathbb{N}$.

Piemērs

$$120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2^3 \cdot 3^1 \cdot 5^1$$

Dalīšana ar atlikumu

Katram $a \in \mathbb{Z}$ un katram $b \in \mathbb{N}$ eksistē viens skaitļu pāris $q, r \in \mathbb{Z}$, lai

$$a = b \cdot q + r.$$

Turklāt $0 \leq r < b$.

Piemērs

Dalot 33 ar 6, iegūstam

$$33 = 6 \cdot 5 + 3.$$

Ievērojam, ka $0 \leq 3 < 6$.

Lielākais kopīgais dalītājs

Divu veselu skaitļu a, b lielākais kopīgais dalītājs $\mathrm{LKD}\,(a, b)$ (vai īsāk – (a, b)) ir lielākais naturālais skaitlis, kas dala gan a, gan b.

Piemērs

$$\mathrm{LKD}\,(54, 27) = (54, 27) = 6$$

Ko darīt, ja gribam atrast lielāko kopīgo dalītāju lieliem skaitļiem, piemēram, $(1092, 595)$? Šādā situācijā var noderēt Eiklīda algoritms.

Eiklīda algoritms

Lai atrastu divu skaitļu $a \leq b$ lielāko kopīgo dalītāju, vispirms a izdala nepilni ar b un tad katrā nākamajā solī iepriekšējās darbības dalītāju nepilni dala ar iegūto atlikumu. Lielākais kopīgais dalītājs ir pēdējais iegūtais nenulles atlikums.

Piemērs

Atradīsim $(1092, 595)$, izmantojot Eiklīda algoritmu.

$$\begin{aligned} 1092 &= 1 \cdot 595 + 497 \\ 595 &= 1 \cdot 497 + 98 \\ 497 &= 5 \cdot 98 + 7 \\ 98 &= 14 \cdot 7 + 0 \end{aligned}$$

Tātad $(1092, 595) = 7$.

Uzdevums

Atrast $(163231, 135749)$.

Polinoma izteiksmes jēdziens

Pieņemsim, ka $\mathbb{K}$ ir skaitļu kopa (varam iztēloties, ka $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, vai $\mathbb{C}$) un x ir patvaļīgs simbols. Katru izteiksmi formā

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

sauc par *polinomu mainīgajā* x *ar koeficientiem no* $\mathbb{K}$, ja $a_i \in \mathbb{K},\ i \in \{1, 2, \ldots, n\}$.

Piemērs

- $4x^3 + 13x - 1$
- x
- 57

Polinoma pakāpe

Par polinoma $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ pakāpi sauc lielāko n, kam $a_n \neq 0$, un apzīmē to ar $\deg a(x) = n$ (no vārda *degree*).

Piemērs

- $4x^3 + 13x - 1$
- x
- 57

Polinomiem ir līdzīgs jēdziens "pirmskaitļiem".

Nereducējami polinomi

Polinomu $a(x)$ sauc par *nereducējamu*, ja neeksistē tādi polinomi $b(x)$ un $c(x)$ ar pozitīvām pakāpēm ($\deg b(x) > 0$ un $\deg c(x) > 0$), lai

$$a(x) = b(x) \cdot c(x).$$

Piemērs

- Polinoms $x - 13$ ir nereducējams;
- Polinoms 57 ir nereducējams;
- Polinoms $x^2 + 1$ ir nereducējams, ja skatāmies uz to kā uz reālu skaitļu polinomu, bet kompleksos skaitļos $x^2 + 1 = (x + i)(x - i)$.

Uzdevums

Sadalīt sekojošos polinomus pirmreizinātājos (nereducējamos polinomos) attiecībā pret $\mathbb{Q}, \mathbb{R}$ un $\mathbb{C}$.

- $x^2 - 3x + 2$
- $x^2 + 4$
- $x^4 - 4$

Līdzīgi kā veseslus skaitļus arī polinomus var dalīt ar atlikumu.

Polinomu dalīšana

Ja $a(x)$ un $b(x)$ ir polinomi un turklāt $b(x) \neq 0$, tad eksistē polinomi $q(x)$ un $r(x)$, lai

$$a(x) = b(x)q(x) + r(x)$$

un

$$\deg r(x) < \deg b(x) \text{ vai } r(x) = 0.$$

Piemērs

Ja $a(x) = x^2$ un $b(x) = x - 2$, tad

$$\underbrace{x^2}_{a(x)} = \underbrace{(x-2)}_{b(x)}\underbrace{(x+2)}_{q(x)} + \underbrace{4}_{r(x)}.$$

Uzdevumi

- Izdalīt $x^2 + 2x - 7$ ar $x - 2$;
- Izdalīt $x^2 + 7x + 6$ ar $x^2 - 5x - 6$;
- Izdalīt $x^3 + x^2 + x + 1$ ar $x^2 + 3x + 2$.

Arī polinomiem mēs varam meklēt lielāko kopīgo dalītāju, izmantojot Eiklīda algoritmu.

Piemērs

Ja $a(x) = x^2 + 7x + 6$ un $b(x) = x^2 - 5x - 6$, atrast (a, b).

$$x^2 + 7x + 6 = (x^2 - 5x - 6) + 12(x + 1)$$
$$x^2 - 5x - 6 = (x + 1)(x - 6) + 0$$

Tā kā $x + 1$ ir pēdējais nenulles atlikums, tad $(a, b) = x + 1$. Tik tiešām

$$x^2 + 7x + 6 = (x + 1)(x + 6)$$
$$x^2 - 5x - 6 = (x + 1)(x - 6)$$

Uzdevums

Atrast (a, b), ja

- $a(x) = x^3 - 5x^2 + 7x - 3$ un $b(x) = 3x^2 - 10x + 7$;
- $a(x) = x^6 - 16$ un $b(x) = x^4 - 2x^3 + 4x - 8$.

Sakņu skaits

Ja $a(x)$ ir nenulles polinoms, tad ar $s_0(a)$ apzīmēsim dažādo sakņu skaitu polinomam a.

Piemērs

Ja $a(x) = (x-1)^2(x+2)^4(x-1)$, tad $s_0(a) = 3$.
Ja $a(x) = (x-1)^{2020}$, tad $s_0(a) = 1$.

Apgalvojums

Ja $a(x)$ ir nenulles polinoms ar kompleksiem koeficientiem, tad ir spēkā vienādība

$$\deg a = \deg(a, a') + s_0(a).$$

Turpmāk visi apskatāmie polinomi būs ņemti ar kompleksiem koeficientiem.

Meisona teorēma

Ja a, b un c ir savstarpēji pirmskaitļi polinomu nozīmē ar pozitīvu pakāpi. Pie tam $a + b = c$, tad

$$\deg a, \deg b, \deg c \leq s_0(abc) - 1.$$

Pierādījums.

Tā kā $a + b = c$, tad $a' + b' = c'$. Pareizinot pirmo vienādojumu ar a' un otro ar a, un atņemot vienu no otra, iegūstam, ka $a'b - ab' = a'c - ac'$. Ievērojam, ka (a, a'), (b, b'), (c, c') dala $a'b - ab'$. Tā kā tie ir savstarpēji pirmskaitļi polinomu nozīmē, secinām, ka

$$(a, a')(b, b')(c, c') | (a'b - ab').$$

Pierādījums (turp.)

$a'b - ab' \neq 0$, jo pretējā gadījumā $a' = b' = c' = 0$, pretrunā ar to, ka a, b, c ir ar pozitīvu pakāpi. Tātad ir spēkā nevienādība

$$\deg(a, a') + \deg(b, b') + \deg(c, c') \leq \deg a + \deg b - 1.$$

Pārnesot visu uz labo pusi un abām pusēm pieskaitot $\deg c$, iegūstam

$$\deg c \leq \deg a - \deg(a, a') + \deg b - \deg(b, b') + \deg c - \deg(c, c') - 1.$$

Pierādījums (turp.)

Pielietojot nevienienādībai apgalvojumu, iegūstam

$$\deg c \leq s_0(a) + s_0(b) + s_0(c) - 1.$$

Tā kā a, b, c ir savstarpēji pirmskaitļi polinomu nozīmē, tad

$$\deg c \leq s_0(abc) - 1,$$

Līdzīgi pierāda pārējos gadījumus. $\square$

Fermā Lielā teorēma polinomiem

Lai $n \geq 3$ būtu naturāls skaitlis. Neeksistē atrisinājums vienādojumam

$$a^n + b^n = c^n,$$

ja a, b, c ir savstarpēji pirmskaitļi polinomu nozīmē ar pozitīvu pakāpi.

Pierādījums.

No Meisona teorēmas izriet, ka

$$\deg a^n \leq s_0(a^n b^n c^n) - 1.$$

Tā kā $\deg a^n = n \cdot \deg a$ un $s_0(a^n) = s_0(a) \leq \deg a$, varam secināt, ka

$$n \cdot \deg a \leq \deg a + \deg b + \deg c - 1.$$

Tādiem pašiem spriedumiem varam iegūt līdzīgas nevienādības polinomiem b un c.

Pierādījums (turp.)

Saskaitot nevienādības

$$n \cdot \deg a \leq \deg a + \deg b + \deg c - 1$$
$$n \cdot \deg b \leq \deg a + \deg b + \deg c - 1$$
$$n \cdot \deg c \leq \deg a + \deg b + \deg c - 1,$$

iegūstam

$$n \cdot \deg abc \leq 3 \deg abc - 3 < \deg abc.$$

Izslēdzot $\deg abc$, iegūstam, ka $n < 3$. Tā kā n ir naturāls skaitlis, tad $n \leq 2$, pierādot teorēmu. □