Полиноми по једној промењивој

Душан Ђукић

Садржај

1° Својства полинома

Моном по промењивој x је израз облика cx^k, где је c константа и k ненегативан цео број. Константа c може бити на пример цео, рационалан, реалан или комплексан број.

Полином по x је збир коначно много монома по x. Другим речима, то је израз облика

$$P(x) = a_n x^n + a_{n-1} + \cdots + a_1 x + a_0. \qquad (*)$$

Ако су у овом изразу само два или три сабирка различита од нуле, онда је P *бином*, односно *трином*.

Константе $a_0, \dots, a_n$ у $(*)$ су *коефицијенти* полинома P. Скуп полинома са коефицијентима у скупу A означавамо са $A[x]$ - тако је нпр. $\mathbb{R}[x]$ скуп полинома са реалним коефицијентима.

У $(*)$ можемо претпоставити без смањења општости да је $a_n \neq 0$ (ако је $a_n = 0$, сабирак $a_n x^n$ се може брисати без мењања полинома). Тада се експонент n назива *степен* полинома P и означава $\deg P$. Специјално, полиноми првог, другог и трећег степена се називају *линеарним*, *квадратним* и *кубним* полиномима. Константни ненула полином има степен 0, док се нула-полиному $P(x) \equiv 0$ додељује степен $-\infty$ из разлога који ће убрзо постати јасни.

- *Пример.* $P(x) = x^3(x+1) + (1-x^2)^2 = 2x^4 + x^3 - 2x^2 + 1$ је полином са целим коефицијентима степена 4.

  $Q(x) = 0x^2 - \sqrt{2}x + 3$ је линеарни полином са реалним коефицијентима.

  $R(x) = \sqrt{x^2} = |x|$, $S(x) = \frac{1}{x}$ и $T(x) = \sqrt{2x+1}$ нису полиноми.

Над полиномима се могу обављати основне рачунске операције. Тако се они могу сабирати, одузимати и множити, при чему ће резултат такође бити полином:

$$
\begin{aligned}
&A(x) = a_0 + a_1x + \cdots + a_nx^n, \quad B(x) = b_0 + b_1x + \cdots + b_mx^m \\
&A(x) \pm B(x) = (a_0 - b_0) + (a_1 - b_1)x + \cdots, \\
&A(x)B(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_mx^{m+n}.
\end{aligned}
$$

Одавде је очигледно како се понашају степени полинома при овим операцијама:

Т.1.1. (i) $\deg(A \pm B) \leq \max(\deg A, \deg B)$, са једнакошћу ако је $\deg A \neq \deg B$.
(ii) $\deg(A \cdot B) = \deg A + \deg B$. $\square$

Конвенција по којој је $\deg 0 = -\infty$ је проистекла управо из овог својства степена, јер једнакост под (ii) не би важила да је другачије.

За разлику од збира, разлике и производа, количник два полинома није обавезно полином. Зато се уместо тога уводи дељење са остатком, слично целим бројевима.

Т.1.2 (Дељење са остатком). Ако су дати полиноми $A(x)$ и $B(x) \neq 0$, тада постоје јединствени полиноми $Q(x)$ и $R(x)$ такви да је

$$A = BQ + R \quad \text{и} \quad \deg R < \deg B.$$

Доказ. Нека је $A(x) = a_nx^n + \cdots + a_0$ и $B(x) = b_kx^k + \cdots + b_0$, при чему је $a_nb_k \neq 0$. Фиксирајмо k и користимо индукцију по n. За $n < k$ тврђење је тривијално; претпоставимо да је $n = N \geq k$ и да тврђење важи за $n < N$. Тада је $A_1(x) = A(x) - \frac{a_n}{b_k}x^{n-k}B(x)$ полином степена мањег од n (јер му је коефицијент уз x^n нула), па по индуктивној претпоставци постоје полиноми Q_1 и R такви да је $A_1 = BQ_1 + R$ и $\deg R$. Међутим, тада је и

$$A = BQ + R, \quad \text{где је} \quad Q(x) = \frac{a_n}{b_k}x^{n-k} + Q_1(x)\,. \;\square$$

Претходно тврђење не важи за полиноме више променљивих - на пример, $A(x, y) = x$ се не може поделити са $B(x, y) = y$ тако да остатак има степен мањи од 1. Ипак, нека друга веома важна својства, као што је нпр. јединствена факторизација, остају на снази и за полиноме више променљивих.

- *Пример.* При дељењу $A(x) = x^3 + x^2 - 1$ са $B(x) = x^2 - x - 3$ количник је $x + 2$, а остатак $5x + 5$, јер је

$$\frac{x^3 + x^2 - 1}{x^2 - x - 3} = x + 2 + \frac{5x + 5}{x^2 - x - 3}\,.$$

Каже се да је полином A *дељив* полиномом B ако је остатак R при дељењу A са B једнак 0, тј. ако постоји полином Q такав да је $A = BQ$.

Т.1.3 (Безуов став). Полином $P(x)$ је дељив биномом $x - a$ ако и само ако је $P(a) = 0$.

Доказ. По дељењу са остатком постоје полином Q и константа c такви да је $P(x) = (x - a)Q(x) + c$. При том је $P(a) = c$, па тврђење постаје очигледно. $\square$

Број a се зове *нула* или *корен* датог полинома $P(x)$ ако је $P(a) = 0$, тј. ако $(x-a) \mid P(x)$.

Наћи нулу полинома f значи решити једначину $f(x) = 0$. То није увек могуће тачно урадити. На пример, доказано је да је то немогуће у општем случају када је f степена 5 или већег. Ипак, нуле полинома се увек могу наћи са произвољном тачношћу. Заправо, f је непрекидна функција, па ако је $f(a) < 0 < f(b)$, тада f има нулу између a и b. Зато је довољно поделити интервал (a, b) на довољно мале интервале - онај у коме f мења знак мора да садржи бар једну нулу.

- *Пример.* Полином $x^2 - 2x - 1$ има две реалне нуле: $x_{1,2} = 1 \pm \sqrt{2}$.

  Полином $x^2 - 2x + 2$ нема реалних нула, али има две комплексне: $x_{1,2} = 1 \pm i$.

  Полином $x^5 - 5x + 1$ има нулу у интервалу $[1.44, 1.441]$ коју не можемо тачно израчунати.

Општије од Безуовог става, важи следеће једноставно тврђење.

Т.1.4. Ако је полином P дељив полиномом Q, онда је свака нула полинома Q уједно и нула полинома P. $\square$

Задатак 1. За које n је полином $x^n + x - 1$ дељив са а) $x^2 - x + 1$, б) $x^3 - x + 1$?

Решење. а) Нуле полинома $x^2 - x + 1$ су $\epsilon_{1,2} = \frac{1 \pm i\sqrt{3}}{2}$. Ако $x^2 - x + 1$ дели $x^n + x - 1$, онда су $\epsilon_{1,2}$ нуле полинома $x^n + x - 1$, тј. $\epsilon_j^n = 1 - \epsilon_j = \epsilon_j^{-1}$ за $j \in \{1, 2\}$, одакле је $\epsilon_j^{n+1} = 1$. Како је $\epsilon_j^k = 1$ ако и само ако $6 \mid k$, одговор је $n \equiv -1 \pmod 6$.

б) Ако $f(x) = x^3 - x + 1$ дели $x^n + x - 1$, дели и $x^n + x^3$. То значи да свака нула полинома $f(x)$ задовољава $x^{n-3} = -1$, а одатле следи да има модул 1. Међутим, $f(x)$ има нулу између -2 и -1 (јер $f(-2) < 0 < f(-1)$) која није модула 1. Дакле, такво n не постоји.

Сваки неконстантан полином са коефицијентима у $\mathbb{C}$ има нулу у скупу комплексних бројева. Ово тврђење ћемо доказати касније, а дотад га користимо "на вересију".

Следеће тврђење је аналогно теореми о јединственој факторизацији природног броја на просте чиниоце.

Т.1.5. Полином $P(x)$ степена $n > 0$ има јединствено представљање у облику

$$P(x) = c(x - x_1)(x - x_2) \cdots (x - x_n),$$

не рачунајући редослед чинилаца, где су $c \neq 0$ и $x_1, \ldots, x_n$ комплексни бројеви, не обавезно различити.

Дакле, полином P има највише $\deg P = n$ различитих нула.

Доказ. Прво докажимо јединственост. Претпоставимо да је

$$P(x) = c(x - x_1)(x - x_2) \cdots (x - x_n) = d(x - y_1)(x - y_2) \cdots (x - y_n).$$

Поређење водећих коефицијената даје $c = d$. Може се сматрати без смањења општости да не постоје i и j за које је $x_i = y_j$ (иначе се чинилац $x - x_i$ може скратити на обе стране). Тада је $P(x_1) = 0$. С друге стране, $P(x_1) = d(x_1 - y_1) \cdots (x_1 - y_n) \neq 0$, контрадикција.

Постојање доказујемо индукцијом по n. Све је јасно ако је $n = 1$. Нека је $n > 1$. Полином $P(x)$ има комплексну нулу, рецимо x_1. По Безуовом ставу је $P(x) = (x - x_1)P_1(x)$ за неки полином P_1 степена $n - 1$. По индуктивној претпоставци постоје комплексни бројеви $x_2, \ldots, x_n$ за које је $P_1(x) = c(x - x_2) \cdots (x - x_n)$, одакле следи $P(x) = c(x - x_1) \cdots (x - x_n)$. $\square$

Последица: Ако полиноми P и Q имају степене не веће од n и узимају једнаке вредности у $n+1$ различитој тачки, онда су они једнаки.

Групишући једнаке чиниоце добијамо *канонску репрезентацију*:

$$P(x) = c(x-a_1)^{\alpha_1}(x-a_2)^{\alpha_2}\cdots(x-a_k)^{\alpha_k},$$

при чему су α_i природни бројеви и $\alpha_1+\cdots+\alpha_k = n$. Број α_i се назива *вишеструкошћу* корена a_i. Вредно је истаћи:

T.1.6. Полином n-тог степена има тачно n комплексних нула бројаних са вишеструкостима. $\square$

Полиноме Q и R зовемо *узајамно простим* ако немају заједничких нула. Ово је еквивалентно услову да не постоји неконстантан полином који дели и Q и R, што је у аналогији са појмом узајамно простих целих бројева. Следеће тврђење одмах следи из претходне теореме:

T.1.7. Ако је полином P дељив узајамно простим полиномима Q и R, онда је дељив полиномом $Q \cdot R$. $\square$

Напомена: То се може доказати без коришћења постојања нула. По Еуклидовом алгоритму примењеном на полиноме постоје полиноми K и L такви да је $KQ+LR = 1$. Ако је $P = QS = RT$ за неке полиноме R, S, онда је $R(KT-LS) = KQS - LRS = S$, одакле $R \mid S$ и $QR \mid QS = P$.

Ако полином $P(x) = a_n x^n + \cdots + a_1 x + a_0$ има реалне коефицијенте и комплексну нулу ξ, тада је $P(\overline{\xi}) = a_n \overline{\xi^n} + \cdots + a_1 \overline{\xi} + a_0 = \overline{P(\xi)} = 0$. Према томе:

T.1.8. Ако је ξ нула реалног полинома $P(x)$, онда је то и $\overline{\xi}$. $\square$

У факторизацији реалног полинома $P(x)$ на линеарне чиниоце можемо да групишемо комплексне нуле по конјугатима:

$$P(x) = c(x-r_1)\cdots(x-r_k)(x-\xi_1)(x-\overline{\xi_1})\cdots(x-\xi_l)(x-\overline{\xi_l}),$$

где су r_i реалне нуле, ξ комплексне и $k+2l = n = \deg P$. Полином $(x-\xi)(x-\overline{\xi}) = x^2 - 2Re\xi + |\xi|^2 = x^2 - p_i x + q_i$ има реалне коефицијенте који задовољавају $p_i^2 - 4q_i < 0$. Доказали смо следеће тврђење:

T.1.9. Реални полином $P(x)$ има јединствену факторизацију (до на редослед чинилаца) у облику

$$P(x) = c(x-r_1)\cdots(x-r_k)(x^2-p_1x+q_1)\cdots(x^2-p_lx+q_l),$$

где су r_i и p_j, q_j реални бројеви са $p_i^2 < 4q_i$ и $k+2l = n$. $\square$

Следи да реалан полином непарног степена увек има непаран број реалних нула (дакле, бар једну).

T.1.10. Ако је $P(x)$ реалан полином који за свако $x \in \mathbb{R}$ узима ненегативну вредност, тада је он представљив у облику збира квадрата два полинома.

Доказ. У факторизацији $P(x)$ на линеарне чиниоце као $c(x-r_1)^{\alpha_1}\cdots(x-a_k)^{\alpha_k}(x-\xi_1)(x-\overline{\xi_1})\cdots(x-\xi_l)(x-\overline{\xi_l})$, сви α_i морају да буду парни и $c > 0$. Осим тога, ако је $(x-\xi_1)\cdots(x-\xi_l) = A(x) - iB(x)$, где су A и B реални полиноми, онда је и $(x-\overline{\xi_1})\cdots(x-\overline{\xi_l}) = A(x) + iB(x)$. Према томе, $(x-\xi_1)(x-\overline{\xi_1})\cdots(x-\xi_l)(x-\overline{\xi_l}) = A(x)^2 + B(x)^2$ и $P(x) = (\sqrt{c}\prod_{i=1}^{k}(x-r_i)^{\alpha_i/2}A(x))^2 + (\sqrt{c}\prod_{i=1}^{k}(x-r_i)^{\alpha_i/2}B(x))^2$. $\square$

Ово тврђење не важи за полиноме више променљивих - видети нпр. задатак 10.

2° **Нуле полинома**

У првој глави смо видели нека основна својства нула полинома. Сада ћемо их додатно испитати, а на крају главе ћемо показати да сваки полином заиста има нулу.

Како су повезани коефицијенти и нуле полинома? Посматрајмо моничан полином

$$P(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = (x - x_1)(x - x_2)\cdots(x - x_n)$$

степена $n > 0$. На пример, упоређивањем коефицијената уз x^{n-1} на обе стране добијамо $x_1 + x_2 + \cdots + x_n = -a_1$; слично, упоређивање слободних коефицијената даје $x_1x_2\cdots x_n = (-1)^n a_n$. Општу везу дају тзв. Вијетове формуле, неколико редова испод.

Елементарни симетрични полиноми по $x_1, \ldots, x_n$ су полиноми $\sigma_1, \sigma_2, \ldots, \sigma_n$, где је

$$\sigma_k = \sigma_k(x_1, x_2, \ldots, x_n) = \sum x_{i_1}x_{i_2}\ldots x_{i_k},$$

при чему се сумира по свим k-точланим подскуповима $\{i_1, \ldots, i_k\}$ од $\{1, 2, \ldots, n\}$.

Између осталог, $\sigma_1 = x_1 + x_2 + \cdots + x_n$ и $\sigma_n = x_1x_2\cdots x_n$. Обично се додефинише $\sigma_0 = 1$ и $\sigma_k = 0$ за $k > n$.

Т.2.1 (Вијетове формуле). Ако су $x_1, x_2, \ldots, x_n$ нуле полинома $P(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$, тада је $a_k = (-1)^k\sigma_k(x_1, \ldots, x_n)$ за $k = 1, 2, \ldots, n$.

Доказ. Индукција по n. Све је јасно за $n = 1$. Претпоставимо да је $n > 1$. Напишимо $P(x) = (x - x_n)Q(x)$, где је $Q(x) = (x - x_1)\cdots(x - x_{n-1})$, и одредимо коефицијент a_k полинома $P(x)$ уз x^k. Како су коефицијенти $Q(x)$ уз x^{k-1} и x^k редом једнаки $a'_{k-1} = (-1)^{k-1}\sigma_{k-1}(x_1, \ldots, x_{n-1})$ и $a'_k = (-1)^k\sigma_k(x_1, \ldots, x_{n-1})$, имамо

$$a_k = -x_na'_{k-1} + a'_k = \sigma_k(x_1, \ldots, x_n). \ \Box$$

- *Пример.* Нуле x_1, x_2, x_3 полинома $P(x) = x^3 - ax^2 + bx - c$ задовољавају $a = x_1 + x_2 + x_3$, $b = x_1x_2 + x_2x_3 + x_3x_1$, $c = x_1x_2x_3$.

Задатак 2. Доказати да полином $x^n + 2nx^{n-1} + 2n^2x^{n-2} + \cdots$ не може да има све реалне нуле.

Решење. Претпоставимо да су све његове нуле $x_1, x_2, \ldots, x_n$ реалне. Оне задовољавају

$$\sum_i x_i = -2n, \quad \sum_{i<j} x_ix_j = 2n^2.$$

Међутим, по неједнакости између средина важи

$$\sum_{i<j} x_ix_j = \frac{1}{2}\left(\sum_i x_i\right)^2 - \frac{1}{2}\sum_i x_i^2 \le \frac{n-1}{2n}\left(\sum_i x_i\right)^2 = 2n(n-1),$$

контрадикција.

Задатак 3. Одредити све полиноме облика $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, где је $a_j \in \{-1, 1\}$ $(j = 0, 1, \ldots, n)$, који имају само реалне нуле.

Решење. Нека су $x_1, \dots, x_n$ нуле датог полинома. Тада је:

$$x_1^2 + x_2^2 + \cdots + x_n^2 = (\sum_i x_i)^2 - 2(\sum_{i<j} x_i x_j) = a_{n-1}^2 - 2a_{n-2} \leq 3;$$
$$x_1^2 x_2^2 \cdots x_n^2 = 1.$$

По неједнакости између средина друга једнакост повлачи $x_1^2 + \cdots + x_n^2 \geq n$, одакле је $n \leq 3$. При том је случај $n = 3$ могућ само ако су $x_1, x_2, x_3 = \pm 1$. Провером лако долазимо до свих решења: $x \pm 1$, $x^2 \pm x - 1$, $x^3 - x \pm (x^2 - 1)$.

Да бисмо доказали да полином нема све реалне нуле, довољна нам је само једна контрадикција. Парадоксално, ако треба да покажемо да полином *има* све реалне нуле, а нисмо у могућности да их све одредимо, ситуација се често усложњава.

Задатак 4. Доказати да су све нуле полинома $f(x) = x(x-2)(x-4)(x-6) + (x-1)(x-3)(x-5)(x-7)$ реалне.

Решење. Како је $f(-\infty) = f(\infty) = +\infty$, $f(1) < 0$, $f(3) > 0$ и $f(5) < 0$, полином f има реалну нулу на сваком од интервала $(-\infty, 1)$, $(1, 3)$, $(3, 5)$, $(5, \infty)$, што је укупно четири.

Као што је већ речено, у неким специјалним случајевима је могуће тачно одредити нуле датог полинома f. Случај полинома степена 1 или 2 је био познат још у старом веку. Позната формула вредна памћења даје решења квадратне једначине $ax^2 + bx + c = 0$ $(a \neq 0)$ у облику

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Израз под кореном $D = b^2 - 4ac$ називамо *дискриминантом* квадратне једначине $ax^2 + bx + c = 0$. Видимо да она има два реална решења ако је $D \geq 0$, и нема реалних решења ако је $D < 0$.

Када је f степена 3 или 4, решење једначине у облику (непрактичних) формула дали су италијански математичари Тартаља и Ферари у 16-том веку. Показаћемо Тартаљин метод решавања кубне једначине.

Пре свега, сменом $x = y - a/3$ сводимо кубну једначину $x^3 + ax^2 + bx + c = 0$ са реалним коефицијентима на једначину облика

$$y^3 + py + q = 0, \quad \text{где је} \quad p = b - \frac{a^2}{3}, \quad q = c - \frac{ab}{3} + \frac{2a^3}{27}.$$

Стављајући $y = u + v$ добијамо једначину $u^3 + v^3 + (3uv + p)y + q = 0$. Међутим, u и v још увек имају један степен слободе, што значи да је дозвољено везати их условом $3uv + p = 0$. Тако наша једначина постаје систем

$$uv = -\frac{p}{3}, \quad u^3 + v^3 = -q$$

који се једноставно решава: u^3 и v^3 су решења квадратне једначине $t^2 + qt - \frac{p^3}{27} = 0$, при чему $uv = -p/3$ мора да буде реално. Тако долазимо до решења:

Т.2.2 (Карданови обрасци). Решења једначине $y^3 + py + q = 0$ са $p, q \in \mathbb{R}$ су

$$y_i = \epsilon^j \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \epsilon^{-j} \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \quad j = 0, 1, 2,$$

где је $\epsilon = \cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3}$ примитивни кубни корен јединице. $\square$

- *Пример.* Једначина $x^3-7x+6=0$ има корен $x=\frac{\sqrt[3]{-9\sqrt{3}+10i}+\sqrt[3]{-9\sqrt{3}-10i}}{\sqrt{3}}$.

  С друге стране, видимо и без Карданове формуле да су корени дате једначине $x_1=1$, $x_2=2$ и $x_3=-3$. Горњи гломазни израз може да представља било који од ова три броја, у зависности од избора вредности трећег корена.

Дискриминанта једначине y^3+py+q је $D=-108\left(\frac{q^2}{4}+\frac{p^3}{27}\right)$. У општем случају, дискриминанта кубне једначине $ax^3+bx^2+cx+d=0$ је

$$D=b^2c^2-4ac^3-4db^3+18abcd-27a^2d^2.$$

Кубна једначина има три реална решења ако је њена дискриминанта D ненегативна; у супротном, она има тачно једно реално решење.

За полином $P(x)=a_nx^n+\cdots+a_0$ n-тог степена са (не обавезно различитим) нулама $x_1,\dots,x_n$, дискриминанта се дефинише као

$$D=a_n^{2n-2}\prod_{i<j}(x_i-x_j)^2.$$

Ова формула је у складу са већ датим дефиницијама за $n=2,3$. Показује се да се D, као симетричан полином по $x_1,\dots,x_n$, може представити као хомоген полином степена $2n-2$ по коефицијентима $a_0,\dots,a_n$. Ако су све нуле x_i реалне, јасно је да је $D\geq 0$. Међутим, за $n\geq 4$ други смер не важи.

Полином $f(x)=a_nx^n+\cdots+a_1x+a_0$ је *симетричан* ако је $a_{n-i}=a_i$ за све i. Ако је $\deg f=n$ непарно, -1 је нула полинома f и полином $f(x)/(x+1)$ је симетричан. Ако је $n=2k$ парно, тада је

$$f(x)/x^k=a_0(x^k+x^{-k})+\cdots+a_{k-1}(x+x^{-1})+a_k$$

полином по $y=x+x^{-1}$, јер је то сваки од израза x^i+x^{-i} (видети 4. задатак у глави 9). Тако је $x^2+x^{-2}=y^2-2$, $x^3+x^{-3}=y^3-3y$, итд. Ово своди једначину $f(x)=0$ на једначину степена $n/2$.

Задатак 5. Доказати да полином $f(x)=x^6-2x^5+x^4-2x^3+x^2-2x+1$ има тачно четири нуле модула 1.

Решење. Ставимо $y=x+x^{-1}$. Тада је

$$\frac{f(x)}{x^3}=g(y)=y^3-2y^2-2y+2.$$

Приметимо да је x модула 1 ако и само ако је $x=\cos t+i\sin t$ за неко t, а тада је $y=2\cos t$; обратно, из $y=2\cos t$ следи $x=\cos t\pm i\sin t$. Другим речима, $|x|=1$ ако и само ако је y реално и $-2\leq y\leq 2$, при чему сваком таквом y одговарају две вредности x ако је $y\neq\pm 2$. Према томе, остаје само да покажемо да $g(y)$ има тачно две реалне нуле у интервалу $(-2,2)$. За то је довољно приметити да је $g(-2)=-10$, $g(0)=2$, $g(2)=-2$, и да према томе g има по једну нулу у сваком од интервала $(-2,0)$, $(0,2)$ и $(2,\infty)$.

3° Полиноми са целим коефицијентима

Посматрајмо полином $P(x)=a_nx^n+\cdots+a_1x+a_0$ са целим коефицијентима. Разлика $P(x)-P(y)$ се може написати у облику

$$a_n(x^n-y^n)+\cdots+a_2(x^2-y^2)+a_1(x-y),$$

у којем су сви сабирци дељиви полиномом $x-y$. Тако долазимо до једноставног али веома важног аритметичког својства полинома из $\mathbb{Z}[x]$:

Т.3.1. Ако је P полином са целим коефицијентима, тада је $P(a) - P(b)$ дељиво са $a - b$ за све различите целе бројеве a и b.

Специјално, све целобројне нуле полинома P деле $P(0)$. $\square$

Важи слично тврђење за рационалне нуле полинома $P(x) \in \mathbb{Z}[x]$.

Т.3.2. Ако је рационалан број p/q ($p, q \in \mathbb{Z}$, $q \neq 0$, нзд$(p, q) = 1$) нула полинома $P(x) = a_n x^n + \cdots + a_0$ са целим коефицијентима, онда $p \mid a_0$ и $q \mid a_n$.

Доказ. Имамо

$$q^n P\left(\frac{p}{q}\right) = a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_0 q^n.$$

Сви сабирци осим можда првог су дељиви са q и сви осим можда последњег су дељиви са p. Према томе, $q \mid a_n p^n$ и $p \mid a_0 q^n$, одакле следи тврђење. $\square$

Задатак 6. Полином $P(x) \in \mathbb{Z}[x]$ узима вредности ± 1 у три различите целобројне тачке. Доказати да он нема целобројних нула.

Решење. Претпоставимо супротно, да су a, b, c, d цели бројеви такви да је $P(a)$, $P(b), P(c) \in \{-1, 1\}$ и $P(d) = 0$. Тада је по претходном тврђењу 1 дељиво различитим целим бројевима $a - d, b - d$ и $c - d$, контрадикција.

Задатак 7. Нека је $P(x)$ полином са целим коефицијентима. Доказати да ако је $P(P(\cdots P(x) \cdots)) = x$ за неки цео број x (где је P примењено n пута), онда $P(P(x)) = x$.

Решење. Посматрајмо низ дат са $x_0 = x$ и $x_{k+1} = P(x_k)$ за $k \geq 0$. Нека је $x_k = x_0$. Знамо да

$$d_i = x_{i+1} - x_i \mid P(x_{i+1}) - P(x_i) = x_{i+2} - x_{i+1} = d_{i+1}$$

за све i, а како је $d_k = d_0$, мора да важи $|d_0| = |d_1| = \cdots = |d_k|$.

Претпоставимо да је $d_1 = d_0 = d \neq 0$. Тада је $d_2 = d$ (у супротном имамо $x_3 = x_1$ те се у низу више никад неће појавити x_0); слично $d_3 = d$, итд, па је $x_k = x_0 + kd \neq x_0$ за све k, контрадикција. Следи да је $d_1 = -d_0$, па је $x_2 = x_0$.

Треба напоменути да полином који у свим целобројним тачкама узима целе вредности није обавезно полином са целим коефицијентима, као што се види на примеру полинома $\frac{x(x-1)}{2}$.

Т.3.3. Ако је вредност полинома $P(x)$ целобројна за сваки цео број x, тада постоје цели бројеви $c_0, \ldots, c_n$ такви да је

$$P(x) = c_n \binom{x}{n} + c_{n-1} \binom{x}{n-1} + \cdots + c_0 \binom{x}{0}.$$

Важи и обратно тврђење.

Доказ. Користимо индукцију по n. За $n = 1$ тврђење је тривијално; нека је $n > 1$. Полином $Q(x) = P(x + 1) - P(x)$ је степена $n - 1$ и узима целе вредонсти у целим тачкама, па по индуктивној претпоставци постоје $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ такви да је

$$Q(x) = a_{n-1} \binom{x}{n-1} + \cdots + a_0 \binom{x}{0}.$$

За свако цело $x > 0$ важи $P(x) = P(0) + Q(0) + Q(1) + \cdots + Q(x-1)$. Користећи једнакост $\binom{0}{k} + \binom{1}{k} + \cdots + \binom{x-1}{k} = \binom{x}{k+1}$ за сваки цео број k добијамо тражено представљање $P(x)$:

$$P(x) = a_{n-1}\binom{x}{n} + \cdots + a_0\binom{x}{1} + P(0). \ \square$$

Задатак 8. Претпоставимо да је, за дати природан број m и полином $R(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $R(x)$ цео број дељив са m кад год је x цео број. Доказати да је тада $n!a_n$ дељиво са m.

Решење. По теореми 3.3 је $\frac{1}{m}R(x) = c_n\binom{x}{n} + c_{n-1}\binom{x}{n-1} + \cdots + c_0\binom{x}{0}$ за неке целе $c_0, \ldots, c_n$. Упоређивање водећег коефицијента на левој и десној страни даје $\frac{c_n}{n!} = \frac{a_n}{m}$, одакле следи тврђење задатка.

4° Нерастављивост полинома

За полином $P(x)$ са целим коефицијентима кажемо да је *нерастављив* или *иредуцибилан* над $\mathbb{Z}[x]$ ако се не може представити у облику производа два неконстантна полинома са целим коефицијентима.

- *Пример.* Сваки полином другог или трећег степена који нема рационалних нула је нерастављив над $\mathbb{Z}$. Такви су нпр. $x^2 - x - 1$ и $2x^3 - 4x + 1$.

Аналогно се дефинише (не)растављивост над скупом полинома са, рецимо, рационалним, реалним или комплексним коефицијентима. Ипак, од наведених, само растављивост над $\mathbb{Z}[x]$ је занимљива. Гаусова лема (доле) тврди да је растављивост над $\mathbb{Q}[x]$ еквивалентна растављивости над $\mathbb{Z}[x]$. Такође, већ смо утврдили да је реалан полином увек растављив на чиниоце у $\mathbb{R}[x]$ степена 1 или 2, док је комплексан полином увек растављив на линеарне чиниоце у $\mathbb{C}[x]$.

Т.4.1 (Гаусова лема). Ако је полином $P(x)$ са целим коефицијентима растављив над $\mathbb{Q}[x]$, онда је он растављив и над $\mathbb{Z}[x]$.

Доказ. Претпоставимо да је $P(x) = a_n x^n + \cdots + a_0 = Q(x)R(x) \in \mathbb{Z}[x]$, где су $Q(x)$ и $R(x)$ неконстантни полиноми са рационалним коефицијентима. Нека су q и r најмањи природни бројеви такви да полиноми $qQ(x) = q_k x^k + \cdots + q_0$ и $rR(x) = r_m x^m + \cdots + r_0$ имају целе коефицијенте. Тада је $qrP(x) = qQ(x) \cdot rR(x)$ разлагање полинома $qrP(x)$ на производ два полинома из $\mathbb{Z}[x]$. Конструисаћемо такво разлагање за $P(x)$.

Нека је p произвољан прост делилац броја q. Сви коефицијенти $P(x)$ су дељиви са p. Нека је i такво да $p \mid q_0, q_1, \ldots, q_{i-1}$ и $p \nmid q_i$. Имамо $p \mid a_i = q_0 r_i + \cdots + q_i r_0 \equiv q_i r_0 \pmod{p}$, одакле $p \mid r_0$. Даље, $p \mid a_{i+1} = q_0 r_{i+1} + \cdots + q_i r_1 + q_{i+1} r_0 \equiv q_i r_1 \pmod{p}$, одакле $p \mid r_1$. Настављајући на овај начин добијамо $p \mid r_j$ за све j. Према томе, $rR(x)/p$ има целе коефицијенте. Овако смо добили разлагање $\frac{rq}{p}P(x)$ на производ полинома из $\mathbb{Z}[x]$. Бирајући друге вредности за p и настављајући овај поступак добијамо жељено разлагање самог полинома $P(x)$. $\square$

Надаље, осим ако другачије нагласимо, под нерастављивошћу подразумевамо нерастављивост над $\mathbb{Z}[x]$.

Задатак 9. Ако су $a_1, a_2, \ldots, a_n$ различити цели бројеви, доказати да је полином $P(x) = (x - a_1)(x - a_2)\cdots(x - a_n) - 1$ иредуцибилан.

Решење. Претпоставимо да је $P(x) = Q(x)R(x)$ за неке неконстантне полиноме $Q, R \in \mathbb{Z}[x]$. Како је $Q(a_i)R(a_i) = -1$ за $i = 1, \ldots, n$, важи $Q(a_i) = 1$ и $R(a_i) = -1$ или $Q(a_i) = -1$ и $R(a_i) = 1$, а у оба случаја је $Q(a_i) + R(a_i) = 0$. Следи да полином $Q(x)+R(x)$ (који очигледно није нула-полином) има n нула $a_1, \ldots, a_n$ што је немогуће јер је његов степен мањи од n.

Т.4.2 (Проширени Ајзенштајнов критеријум). Нека је $P(x) = a_n x^n + \cdots + a_1 x + a_0$ полином са целим коефицијентима. Ако постоје прост број p и цео број $k \in \{0, 1, \ldots, n-1\}$ такав да

$$p \mid a_0, a_1, \ldots, a_k, \ \ p \nmid a_{k+1} \ \text{ и } \ p^2 \nmid a_0,$$

тада $P(x)$ има нерастављиви фактор степена већег од k.

Специјално, ако се p може узети тако да је $k = n - 1$, тада је $P(x)$ нерастављив.

Доказ. Слично доказу Гаусове леме. Претпоставимо да је $P(x) = Q(x)R(x)$, где су $Q(x) = q_k x^k + \cdots + q_0$ и $R(x) = r_m x^m + \cdots + r_0$ полиноми из $\mathbb{Z}[x]$. Како је $a_0 = q_0 r_0$ дељиво са p, а није са p^2, тачно један од q_0, r_0 је дељив са p. Нека $p \mid q_0$ и $p \nmid r_0$. Сада, $p \mid a_1 = q_0 r_1 + q_1 r_0$, одакле $p \mid q_1 r_0$, тј. $p \mid q_1$, и тако даље. Овако закључујемо да су сви коефицијенти $q_0, q_1, \ldots, q_k$ дељиви са p, али $p \nmid q_{k+1}$. Следи да је $\deg Q \geq k + 1$.

Задатак 10. За цео број $n > 1$ посматрајмо полином $f(x) = x^n + 5x^{n-1} + 3$. Доказати да не постоје полиноми $g(x), h(x)$ са целим коефицијентима и степеном већим од 0 такви да је $f(x) = g(x)h(x)$.

Решење. По (проширеном) Ајзенштајновом критеријуму, f има иредуцибилни фактор чији је степен бар $n - 1$. Како f нема целобројних нула, мора бити иредуцибилан.

Задатак 11. Ако је p прост број, доказати да је полином $\Phi_p(x) = x^{p-1} + \cdots + x + 1$ иредуцибилан.

Решење. Уместо $\Phi_p(x)$ посматраћемо $\Phi_p(x+1)$ и показаћемо да је он иредуцибилан. Одатле јасно следи тврђење. Имамо

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{p-1} x^{p-2} + \cdots + \binom{p}{2} x + p.$$

Овај полином задовољава све претпоставке Ајзенштајновог критеријума на основу којег је иредуцибилан.

Понекад је у испитивању растављивости неког полинома од користи испитати његове нуле и њихове модуле. Следећи задаци то добро илуструју.

Задатак 12. Доказати да је полином $P(x) = x^n + 4$ растављив над $\mathbb{Z}[x]$ ако и само ако је n дељиво са 4.

Решење. Све нуле полинома P имају једнак модул $2^{2/n}$. Ако су Q и R полиноми из $\mathbb{Z}[x]$ и $\deg Q = k$, тада је $|Q(0)|$ производ модула нула полинома Q и једнак је $2^{2k/n}$, и пошто је то цео број, закључујемо да је $n = 2k$.

Ако је k непарно, полином Q има реалну нулу, што је немогуће јер $P(x)$ нема реалних нула. Дакле, $2 \mid k$ и $4 \mid n$.

Онда када се нуле не могу тачно одредити, треба наћи довољно добру оцену. Проценити комплексну нулу полинома није увек једноставно. Главно оруђе које нам је при руци је неједнакост троугла између комплексних бројева:

$$|x| - |y| \leq |x + y| \leq |x| + |y|.$$

Посматрајмо полином $P(x) = a_n x^n + a_{n-k} xn - k + \cdots + a_1 x + a_0$ са комплексним коефицијентима ($a_n \neq 0$). Нека је α његова нула. Ако је M реалан број такав да је $|a_i| < M|a_n|$ за све i, важи

$$0 = |P(\alpha)| \geq |a_n||\alpha|^n - M|a_n|(|\alpha|^{n-k} + \cdots + |\alpha| + 1) > |a_n||\alpha|^n \left(1 - \frac{M}{|\alpha|^{k-1}(|\alpha| - 1)}\right),$$

одакле је $|\alpha|^{k-1}(|\alpha| - 1) < M$. Тако долазимо до једне оцене:

Т.4.3. Нека је $P(x) = a_n x^n + \cdots + a_0$ комплексан полином са $a_n \neq 0$ и $M = \max\limits_{0 \leq k < n} \left|\frac{a_k}{a_n}\right|$. Ако је $a_{n-1} = \cdots = a_{n-k+1} = 0$, тада су сви корени полинома P по модулу мањи од $1 + \sqrt[k]{M}$.

Специјално, у случају $k = 1$, свака нула полинома $P(x)$ је по модулу мања од $M + 1$. □

Задатак 13. Ако је $\overline{a_n \ldots a_1 a_0}$ декадни запис простог броја и $a_n > 1$, доказати да је полином $P(x) = a_n x^n + \cdots + a_1 x + a_0$ нерастављив. (*БМО 1989.2*)

Решење. Претпоставимо да су Q и R неконстантни полиноми из $\mathbb{Z}[x]$ са $Q(x)R(x) = P(x)$. Нека су $x_1, \ldots, x_k$ нуле полинома Q и $x_{k+1}, \ldots, x_n$ нуле R. По услову задатка је $P(10) = Q(10)R(10)$ прост број, па можемо без смањења општости сматрати да је

$$|Q(10)| = (10 - x_1)(10 - x_2) \cdots (10 - x_k) = 1.$$

Међутим, по теореми о процени корена, свака нула x_i је по модулу мања од $1 + 9/2 = 11/2 < 9$; према томе $|10 - x_i| > 1$ за све i, што горњу једнакост чини немогућом.

Задатак 14. Нека је $p > 2$ прост број и нека је $P(x) = x^p - x + p$.

(а) Доказати да су све нуле полинома P по модулу мање од $p^{\frac{1}{p-1}}$.

(б) Доказати да је полином $P(x)$ иредуцибилан.

Решење. (а) Нека је y нула полинома P. Тада је $|y|^p - |y| \leq |y^p - y| = p$. Одавде следи да ако је $|y| \geq p^{\frac{1}{p-1}}$, онда је

$$|y|^p - |y| \geq (p - 1)p^{\frac{1}{p-1}} > p,$$

што је контрадикција. Овде смо користили неједнакост $p^{\frac{1}{p-1}} > \frac{p}{p-1}$ која следи нпр. из биномног развоја $p^{p-1} = ((p - 1) + 1)^{p-1}$.

(б) Претпоставимо да је $P(x)$ производ два неконстантна полинома $Q(x)$ и $R(x)$ са целим коефицијентима. Један од ова два полинома, рецимо Q, има слободан члан једнак $\pm p$. С друге стране, нуле $x_1, \ldots, x_k$ полинома Q задовољавају $|x_1|, \ldots, |x_k| < p^{\frac{1}{p-1}}$ на основу дела (а), и $x_1 \cdots x_k = \pm p$, одакле следи да је $k \geq p$, а то је немогуће.

5° **Интерполација полинома**

Полином n-тог степена чије су вредности дате у $n+1$ тачака једнозначно је одређен. Његово одређивање назива се *интерполација*. Претпоставимо, дакле, да је P полином n-тог степена и да је дато $P(x_i) = y_i$ у различитим тачкама $x_0, x_1, \ldots, x_n$. Постоје јединствени полиноми $E_0, E_1, \ldots, E_n$ n-тог степена такви да је $E_i(x_i) = 1$ и $E_i(x_j) = 0$ за $j \neq i$. Тада полином

$$P(x) = y_0E_0(x) + y_1E_1(x) + \cdots + y_nE_n(x)$$

има тражене особине: заиста, $P(x_i) = \sum_j y_jE_j(x_i) = y_iE_i(x_i) = y_i$. Преостаје још само да се пронађу одговарајући полиноми $E_0, \ldots, E_n$. Полином који се анулира у n тачака x_j, $j \neq i$, дељив је са $\prod_{j\neq i}(x-x_j)$, и сад лако добијамо $E_i(x) = \prod_{j\neq i} \frac{(x-x_j)}{(x_i-x_j)}$. Тако смо добили:

T.5.1 (Лагранжов интерполациони полином). За дате бројеве $y_0, \ldots, y_n$ и различите $x_0, \ldots, x_n$ постоји јединствен полином $P(x)$ n-тог степена такав да је $P(x_i) = y_i$ за $i = 0, 1, \ldots, n$ и он је дат формулом

$$P(x) = \sum_{i=0}^{n} y_i \prod_{j\neq i} \frac{(x-x_j)}{(x_i-x_j)}. \ \Box$$

- *Пример.* Наћи кубни полином Q такав да је $Q(i) = 2^i$ за $i = 0, 1, 2, 3$.

  Решење. $Q(x) = \frac{(x-1)(x-2)(x-3)}{-6} + \frac{2x(x-2)(x-3)}{2} + \frac{4x(x-1)(x-3)}{-2} + \frac{8x(x-1)(x-2)}{6} = \frac{x^3+5x+6}{6}$.

Да би се израчунала вредност полинома у некој тачки, понекад није потребно рачунати Лагранжов полином. Лагранжов полином заправо има непријатну особину да даје одговор у запетљаном облику.

- *Пример.* Ако полином P n-тог степена узима вредност 1 у тачкама $0, 2, 4, \ldots, 2n$, израчунати $P(-1)$.

  Решење. $P(x)$ је наравно идентички једнак 1, и $P(-1) = 1$. Али ако применимо Лагранжов полином, ево шта ћемо добити:

$$P(-1) = \sum_{i=0}^{n}\prod_{j\neq i}\frac{1-2i}{(2j-2i)} = \sum_{i=0}^{n}\prod_{j\neq i}\frac{-1-2j}{(2i-2j)} = \frac{(2n+1)!!}{2^n}\sum_{i=0}^{n}\frac{(-1)^{n-i}}{(2i+1)i!(n-i)!}\ .$$

Уместо тога, често је корисно посматрати *коначну разлику* полинома P која се дефинише као $P^{[1]}(x) = P(x+1) - P(x)$ и која је степена за 1 мањег него P. Даље дефинишемо k-ту коначну разлику, $P^{[k]} = (P^{[k-1]})^{[1]}$, која има степен $n-k$ (где је $n = \deg P$). Општи облик $P^{[k]}$ је

$$P^{[k]}(x) = \sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}P(x+i),$$

што се показује једноставном индукцијом. Између осталог, $P^{[n]}$ је константно и $P^{[n+1]} = 0$, одакле добијамо једнакости

T.5.2. $P(x+n+1) = P(x+n) + \sum_{i=1}^{n} P^{[i]}(x+n-i) = \sum_{i=0}^{n}(-1)^{n-i}\binom{n+1}{i}P(x+i).\ \Box$

Задатак 15. Полином P степена n задовољава $P(i) = \binom{n+1}{i}^{-1}$ за $i = 0, 1, \ldots, n$. Одредити $P(n+1)$.

Решење. Имамо

$$0 = \sum_{i=0}^{n+1} (-1)^i \binom{n+1}{i} P(i) = (-1)^{n+1} P(n+1) + \begin{cases} 1, & 2 \mid n; \\ 0, & 2 \nmid n. \end{cases}$$

Следи да је $P(n+1) = \begin{cases} 1, & 2 \mid n; \\ 0, & 2 \nmid n. \end{cases}$

Задатак 16. Ако је $P(x)$ полином парног n-тог степена, $P(0) = 1$ и $P(i) = 2^{i-1}$ за $i = 1, \ldots, n$, доказати да је $P(n+2) = 2P(n+1) - 1$.

Решење. Видимо да је $P^{[1]}(0) = 0$ и $P^{[1]}(i) = 2^{i-1}$ за $i = 1, \ldots, n-1$; даље је $P^{[2]}(0) = 1$ и $P^{[2]}(i) = 2^{i-1}$ за $i = 1, \ldots, n-2$, итд. Уопште, лако се види да важи $P^{[k]}(i) = 2^{i-1}$ за $i = 1, \ldots, n-k$ и $P^{[k]}(0)$ је 0 ако је k непарно и 1 ако је парно. Сада је

$$P(n+1) = P(n) + P^{[1]}(n) = \cdots = P(n) + P^{[1]}(n-1) + \cdots + P^{[n]}(0) = \begin{cases} 2^n, & 2 \mid n; \\ 2^n - 1, & 2 \nmid n. \end{cases}$$

Слично, $P(n+2) = 2^{2n+1} - 1$.

6° Извод полинома

Првих пар редова искористићемо да поновимо најосновније чињенице диференцијалног рачуна.

Извод реалне или комплексне функције f дефинисане на подскупу $\mathbb{R}$ (или $\mathbb{C}$) у тачки a, ако постоји, је $f'(a) = \lim_{t \to 0} \frac{f(a+t) - f(a)}{t}$ - тада кажемо да је f *диференцијабилна* у a. За произвољне диференцијабилне функције f и g и $c \in \mathbb{R}$ важи

$$(cf)' = cf'; \quad (f+g)' = f' + g'; \quad (fg)' = f'g + fg'; \quad \left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2}$$
$$f(g(x))' = f'(g(x))g'(x); \quad (\ln f)' = \frac{f'}{f}.$$

Полином $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ је диференцијабилан у свакој тачки, и његов извод је дат изразом

$$P'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1.$$

Обрнута операција, неодређени интеграл, је дата изразом

$$\int P(x)dx = \frac{a_n}{n+1} x^{n+1} + \frac{a_{n-1}}{n} x^n + \cdots + a_0 x + C.$$

Изводи добро апроксимирају ток функције у околини дате тачке, као што се види из *Тејлоровог развоја* функције f:

Т.6.1. Ако је функција $f(x)$ n пута непрекидно диференцијабилна у тачки a, у некој околини тачке a (за мало t) важи

$$f(a+t) = f(a) + f'(a)t + \frac{f''(a)}{2!} t^2 + \cdots + \frac{f^{(n)}(a)}{n!} t^n + o(t^n). \ \square$$

Специјално, ако је f полином степена n, члан $o(t^n)$ је идентички једнак нули.

Следеће тврђење такође важи за све диференцијабилне функције.

Т.6.2 (Ролова теорема). Између сваке две реалне нуле реалног полинома $P(x)$ налази се бар једна нула полинома $P'(x)$.

Последица. Ако $P(x)$ има све реалне нуле, онда и $P'(x)$ има све реалне нуле.

Доказ. Нека су $a < b$ две нуле полинома P, нека је без смањења општости $P'(a) > 0$ и нека је c тачка интервала $[a, b]$ у којој P узима максималну вредност (таква тачка постоји јер је интервал $[a, b]$ компактан). Знамо да важи $P(x) = P(c) + (x - c)[P'(c) + o(1)]$. Ако је нпр. $P'(c) > 0$ (случај $P'(c) < 0$ слично води контрадикцији), важило би $P(x) > P(c)$ у некој малој околини c, што је контрадикција. Могуће је једино $P'(c) = 0$, па је c нула полинома $P'(x)$ између a и b. $\square$

Сада ћемо дати обећани доказ тврђења да сваки полином има комплексну нулу. Ова веома важна теорема има више доказа, од којих већина користи основне чињенице из комплексне анализе или топологије.

Т.6.3 (Основна теорема алгебре). Сваки неконстантни комплексни полином $P(x)$ има нулу у скупу комплексних бројева.

Доказ. Нека је $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. За довољно велико R, на пример $R > 1 + 2|a_0| + |a_1| + \cdots + |a_{n-1}|$, у свим тачкама x са $|x| = R$ имамо $|P(x)| \geq |x^n| - |a_{n-1}x^{n-1} + \cdots + a_0| > |a_0|$. Посматрајмо непрекидну функцију $|P(x)|$ на компактном скупу $\{x \in \mathbb{C} \mid |x| \leq R\}$. По теореми о екстремној вредности, она достиже своју минималну вредност на том скупу у некој тачки c, и она задовољава $|c| < R$. Показаћемо да је $P(c) = 0$.

Претпоставимо да је $|P(c)| > 0$ и нека је $P'(c) \neq 0$. Како је $P(c + t) = P(c) + tP'(c) + o(t)$, одаберимо t у правцу количника $-P(c)/P'(c)$, тј. $t = -rP(c)/P'(c)$ за неко $r > 0$, $r \in \mathbb{R}$. Тада је $P(c + t) = (1 - r)P(c) + o(r)$, што је мање од $P(c)$ за довољно мало r, а то је контрадикција.

На сличан начин поступамо и ако је $P'(c) = 0$. Нека је $P'(c) = \cdots = P^{(k-1)}(c) = 0 \neq P^{(k)}(c)$. Приметимо да такво k постоји, јер је нпр. $P^{(n)}(c) = n!a_n \neq 0$. Тада је по Тејлоровом развоју $P(c + t) = P(c) + P^{(k)}(c)t^k/k! + o(t^k)$. Ако одаберемо t такво да је $t^k = -rP(c)/P^{(k)}(c)$ за неко $r > 0$, $r \in \mathbb{R}$, имаћемо $P(c + t) = (1 - r)P(c) + o(r)$, што је опет мање од $P(c)$ за довољно мало r, контрадикција. $\square$

Онда када полином P није задат помоћу коефицијената већ канонски, као $P(x) = (x - x_1)^{k_1} \cdots (x - x_n)^{k_n}$, погоднији израз за извод се добија коришћењем правила за логаритамски извод или извод производа:

$$P'(x) = P(x)\left(\frac{k_1}{x - x_1} + \cdots + \frac{k_n}{x - x_n}\right).$$

Слична формула се може добити и за други извод.

Задатак 17. Претпоставимо да реални бројеви $0 = x_0 < x_1 < \cdots < x_n < x_{n+1} = 1$ задовољавају

$$\sum_{j=0,\, j\neq i}^{n+1} \frac{1}{x_i - x_j} = 0 \quad \text{за } i = 1, 2, \ldots, n. \tag{1}$$

Доказати да важи $x_{n+1-i} = 1 - x_i$ за $i = 1, 2, \ldots, n$.

Решење. Нека је $P(x) = (x-x_0)(x-x_1)\cdots(x-x_n)(x-x_{n+1})$. Имамо

$$P'(x) = \sum_{j=0}^{n+1} \frac{P(x)}{x-x_j} \quad \text{и} \quad P''(x) = \sum_{j=0}^{n+1} \sum_{k \neq j} \frac{P(x)}{(x-x_j)(x-x_k)} \ .$$

Одатле је

$$P''(x_i) = 2P'(x_i) \sum_{j \neq i} \frac{1}{(x_i - x_j)}$$

за $i = 0, 1, \ldots, n+1$, па из услова следи $P''(x_i) = 0$ за $i = 1, 2, \ldots, n$. Отуда

$$x(x-1)P''(x) = (n+2)(n+1)P(x).$$

Лако се види да постоји јединствен моничан полином степена $n+2$ који задовољава горњу диференцијалну једначину - довољно је упоредити коефицијенте на обе стране једначине. С друге стране, полином $Q(x) = (-1)^n P(1-x)$ такође задовољава ту једначину и моничан је, степена $n+2$, па мора бити $(-1)^n P(1-x) = P(x)$, одакле следи тврђење.

Оно што даје изводу полинома посебну употребну вредност јесте његово чување вишеструких нула полинома.

Т.6.4. Ако $(x-\alpha)^k \mid P(x)$, онда $(x-\alpha)^{k-1} \mid P'(x)$.

Доказ. Ако је $P(x) = (x-\alpha)^k Q(x)$, онда је $P'(x) = (x-\alpha)^k Q'(x) + k(x-\alpha)^{k-1}Q(x)$. $\square$

Задатак 18. Одредити реални полином $P(x)$ степена највише 5 такав да $P(x)$ даје редом остатке -1 и 1 при дељењу са $(x-1)^3$ и $(x+1)^3$.

Решење. Ако $P(x)+1$ има троструку нулу у тачки 1, онда његов извод $P'(x)$ има двоструку нулу у тој тачки. Слично, $P'(x)$ има двоструку нулу и у тачки -1. Следи да је $P'(x)$ дељиво полиномом $(x-1)^2(x+1)^2$. Међутим, $P'(x)$ је степена највише 4, одакле је

$$P'(x) = c(x-1)^2(x+1)^2 = c(x^4 - 2x^2 + 1)$$

за неку константу c. Сада је $P(x) = c(\frac{1}{5}x^5 - \frac{2}{3}x^3 + x) + d$ за неке реалне бројеве c и d. Из услова $P(-1) = 1$ и $P(1) = -1$ добијамо $c = -15/8$, $d = 0$ и

$$P(x) = -\frac{1}{8}(3x^5 - 10x^3 + 15x).$$

Задатак 19. За дате полиноме $P(x)$ и $Q(x)$ и произвољно $k \in \mathbb{C}$, означимо

$$P_k = \{z \in \mathbb{C} \mid P(z) = k\} \quad \text{и} \quad Q_k = \{z \in \mathbb{C} \mid Q(z) = k\}.$$

Ако је $P_0 = Q_0$ и $P_1 = Q_1$, доказати да мора бити $P(x) = Q(x)$.

Решење. Претпоставићемо без смањења општости да је $n = \deg P \geq \deg Q$. Нека је $P_0 = \{z_1, z_2, \ldots, z_k\}$ и $P_1 = \{z_{k+1}, z_{k+2}, \ldots, z_{k+m}\}$. Полиноми P и Q се поклапају у $k+m$ тачака $z_1, z_2, \ldots, z_{k+m}$. Наш резултат ће следити ако покажемо да је $k+m > n$.

По услову је

$$P(x) = (x-z_1)^{\alpha_1} \cdots (x-z_k)^{\alpha_k} = (x-z_{k+1})^{\alpha_{k+1}} \cdots (x-z_{k+m})^{\alpha_{k+m}} + 1$$

за неке природне бројеве $\alpha_1, \ldots, \alpha_{k+m}$. Посматрајмо $P'(x)$. Знамо да је он дељив са $(x - z_i)^{\alpha_i - 1}$ за $i = 1, 2, \ldots, k + m$; дакле,

$$\prod_{i=1}^{k+m} (x - z_i)^{\alpha_i - 1} \mid P'(x).$$

Одатле имамо $2n-k-m = \deg \prod_{i=1}^{k+m}(x-z_i)^{\alpha_i-1} \leq \deg P' = n-1$, тј. $k+m \geq n+1$, што смо и желели.

Исту идеју можемо да искористимо и у доказу следећег занимљивог тврђења које се показало веома корисним у доказивању да неке диофантске једначине за полиноме немају решења.

Т.6.5 (Мејсон). Ако су A, B и C узајамно прости полиноми са $A + B = C$, онда је степен сваког од полинома A, B, C мањи од броја различитих нула полинома ABC.

Доказ. Нека је

$$A(x) = \prod_{i=1}^{k} (x - p_i)^{a_i}, \quad B(x) = \prod_{i=1}^{l} (x - q_i)^{b_i}, \quad C(x) = \prod_{i=1}^{m} (x - r_i)^{c_i}.$$

Напишимо дату једнакост као $A(x)/C(x) + B(x)/C(x) = 1$ и диференцирајмо је по x. Добијамо

$$\frac{A(x)}{C(x)} \left(\sum_{i=1}^{k} \frac{a_i}{x - p_i} - \sum_{i=1}^{m} \frac{c_i}{x - r_i} \right) = -\frac{B(x)}{C(x)} \left(\sum_{i=1}^{l} \frac{b_i}{x - q_i} - \sum_{i=1}^{m} \frac{c_i}{x - r_i} \right),$$

из чега видимо да се $A(x)/B(x)$ може представити као количник два полинома степена не већег од $k + l + m - 1$. Тврђење следи из чињенице да су A и B узајамно прости. $\square$

Ово тврђење је нека врста полиномског еквивалента такозване ABC-хипотезе[1], отвореног проблема из теорије бројева. Следеће тврђење је очигледно еквивалент Велике Фермаове Теореме за полиноме:

Т.6.6. Ако постоје узајамно прости полиноми P, Q, R са комплексним коефицијентима такви да је

$$P^a + Q^b = R^c,$$

где су a, b, c природни бројеви, тада важи $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} > 1$.

Доказ. Применимо теорему 6.5 на полиноме P^a, Q^b, R^c. Сваки од $a \deg P$, $b \deg Q$, $c \deg R$ је мањи од $\deg P + \deg Q + \deg R$, одакле је $\frac{1}{a} > \frac{\deg P}{\deg P + \deg Q + \deg R}$, итд. Сабирањем добијамо тражену неједнакост. $\square$

Последица: Једначина $P^n + Q^n = R^n$ нема решења у узајамно простим полиномима за природан број $n > 2$. $\square$

Може се показати да у Т.6.6 важи и други смер: ако је $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} > 1$, онда једначина има решења. На пример, за $(a, b, c) = (2, 4, 3)$ имамо решење $P(x) = x^{12} - 33x^8 - 33x^4 + 1$, $Q(x) = \sqrt[4]{108}(x^5 - x)$, $R(x) = x^8 + 14x^4 + 1$.

[1] ABC-*хипотеза:* За свако $\varepsilon > 0$ постоји константа $K > 0$ таква да је, за све узајамно просте целе бројеве a, b, c са $a + b = c$, производ свих различитих простих делилаца броја abc већи од $Kc^{1-\varepsilon}$.

7° Број нула полинома

Примена својстава извода нам може помоћи да оценимо број нула датог реалног полинома на одређеном интервалу. Показаћемо две класичне теореме о броју нула.

Т.7.1. Нека је $P(x)$ реалан полином степена n. Са $N(x)$ означавамо број промена знака у низу $P(x), P'(x), \dots, P^{(n)}(x)$. Ако је $a < b$, тада број нула полинома P (бројаних са многустукостима) на интервалу (a, b) није већи од $N(a) - N(b)$.

Доказ. Пошто су полиноми непрекидне функције, при непрекидном проласку x од a до b, $N(x)$ се може променити само у нули неког од полинома $P(x), P'(x), \dots$.

Испитајмо понашање броја $N(x)$ у околини нуле x_0 полинома P. Нека је $P(x) = (x - x_0)^r Q(x)$, $Q(x_0) \neq 0$. Како је $P'(x) = r(x - x_0)^{r-1}Q(x) + (x - x_0)^r Q'(x) = (x-x_0)^{r-1}(rQ(x)+(x-x_0)Q'(x)) \sim r(x-x_0)^{r-1}Q(x)$, у некој околини тачке x_0 $P'(x)$ је истог знака као $(x - x_0)^{r-1}Q(x_0)$. Слично добијамо да је, за $k \leq r$, $P^{(k)}(x)$ у некој околини тачке x_0 истог знака као $(x - x_0)^{r-k}Q(x_0)$. У низу $(x - x_0)^{r-k}$, $k = 0, \dots, r$ има r промена знака за $x < x_0$ и ниједна промена за $x > x_0$, па се тако број промена знака у делу низа $P(x), \dots, P^{(r)}(x)$ при проласку x кроз x_0 смањио за r.

Нека је сада x_0 r-тострука нула полинома $P^{(i)}$ која није нула полинома $P^{(i-1)}$, $i \geq 1$. Сличним резоновањем добијамо да су $P^{(i-1)}(x), P^{(i)}(x), \dots, P^{(i+r)}(x)$ у некој околини тачке x_0 истог знака као $A, (x - x_0)^r B, \dots, B$, где је $A = P^{(i-1)}(x_0)$ и $B = P^{(i+r)}(x_0)$. Тако се за парно r број промена знака у овом делу низа смањио за r, а за непарно r тај број се смањио за $r \pm 1$, тј. опет за паран број.

Следи да се, при проласку x кроз r-тоструку нулу полинома $P(x)$, $N(x)$ смањује за број исте парности као r и не мањи од r, док се у сваком другом случају $N(x)$ или не мења или смањује за паран број, одакле следи тврђење. □

Т.7.2 (Декартово правило). Број позитивних нула реалног полинома $P(x) = a_n x^n + \dots + a_1 x + a_0$ није већи од броја промена знака у низу $a_n, \dots, a_1, a_0$.

Доказ. У ознакама из претходне теореме, $P^{(k)}(0) = k! a_k$, па је $N(0)$ једнако броју промена знака у низу $a_n, \dots, a_1, a_0$, док је $N(b) = 0$ за довољно велико b, па из претходне теореме следи тврђење. □

Нека је $P(x)$ реалан полином. Дефинишимо низ полинома P_i примењујући Еуклидов алгоритам на $P_0 = P$ и $P_1 = P'$: за $k \geq 1$, ако је $R(x)$ остатак при дељењу полинома $P_{k-1}(x)$ са $P_k(x)$, $\deg R < \deg P_k$, ставимо $P_{k+1} = -R(x)$. Овај алгоритам се очигледно завршава у коначном броју корака. *Штурмов низ* је низ полинома $P_0, P_1, \dots, P_m$, где је $P_{m+1} = 0 \neq P_m$. Примећујемо да је P_m највећи (у односу на степен) заједнички делилац полинома P и P'.

Ако $P(x)$ има вишеструку нулу x_0, тада су и P_0 и P_1, а самим тим и сви P_i, дељиви са $x - x_0$, те је $P_m(x)$ неконстантан полином.

С друге стране, ако $P(x)$ нема вишеструких нула, полиноми P и P' су узајамно прости (заиста, ако имају заједничку нулу x_0, онда је x_0 бар двострука нула полинома P), тако да је P_m ненула константа. Исто тако видимо и да никоја два узастопна члана Штурмовог низа немају заједничку нулу.

Т.7.3 (Штурмова теорема). Нека је $P(x)$ реалан полином без вишеструких нула. Означимо са $Z(x)$ број промена знака (не рачунајући нуле) у низу $P(x) =$

$P_0(x), P_1(x), \ldots, P_m(x)$. Тада је број нула полинома $P(x)$ на интервалу $(a, b]$, $a < b$, једнак $N(a) - N(b)$.

Доказ. Довољно је посматрати понашање Штурмовог низа у околини нула његових чланова-полинома.

Нека је ξ нула неког полинома P_i, $0 < i < m$. Тада су $P_{i-1}(\xi)$ и $P_{i+1}(\xi)$ различити од нуле и различитог знака. Према томе, у низу $P_{i-1}(x), P_i(x), P_{i+1}(x)$ за x у околини ξ имамо тачно једну промену знака са обе стране ξ, па се $Z(x)$ не мења када x пролази кроз ξ.

Број $Z(x)$ се може променити само при проласку x кроз неку нулу ξ полинома P. Знамо да је тада $P_1(\xi) \neq 0$. Ако је $P_1(\xi) = P'(\xi) > 0$, $P(x)$ је растуће у ξ и мења знак из негативног у позитиван, тако да се $Z(x)$ смањује за 1. Слично, $Z(x)$ се такође смањује за 1 у тачки ξ ако је $P_1(\xi) < 0$. Овим је тврђење доказано. □

- *Пример.* Нека је $P(x) = P_0(x) = x^4 - 3x^2 + 2x - 3$. Тада је:

$$\begin{aligned} P_1(x) = &\quad 4x^3 - 6x + 2, \\ P_2(x) = &\quad -(P_0(x) - \tfrac{1}{4}xP_1(x)) = \tfrac{3}{2}x^2 + \tfrac{3}{2}x + 3, \\ P_3(x) = &\quad -(P_1(x) - (\tfrac{8}{3}x - \tfrac{8}{3})P_2(x)) = 10x - 10, \\ P_4(x) = &\quad -(P_2(x) - (\tfrac{3}{20}x + \tfrac{3}{10})P_3(x) = -10. \end{aligned}$$

Интервал $(0, 2]$ садржи тачно једну нулу $P(x)$. Заиста, $(P_0(0), P_1(0), P_2(0), P_3(0), P_4(0)) = (-3, 2, 3, -10, -10)$ и $(P_0(2), P_1(2), P_2(2), P_3(2), P_4(2)) = (5, 22, 12, 10, -10)$, па је $Z(0) - Z(2) = 2 - 1 = 1$.

С друге стране, у $(2, \infty)$ нема нула, јер за свако довољно велико x важи $P_0(x), P_1(x), P_2(x), P_3(x) > 0 > P_4(x)$, па је $Z(+\infty) = \lim_{x \to +\infty} Z(x) = 1$.

8° Симетрични полиноми

Симетричан полином по променљивим $x_1, \ldots, x_n$ је сваки полином који се не мења пермутовањем индекса променљивих. На пример, полином x_1^2 је симетричан по x_1 (што и није неко чудо), али није симетричан по x_1, x_2 јер се заменом места индексима 1 и 2 мења у полином x_2^2.

Дефиниција. Полином $P(x_1, x_2, \ldots, x_n)$ је *симетричан* ако за сваку пермутацију π скупа $\{1, 2, \ldots, n\}$ важи $P(x_1, x_2, \ldots, x_n) \equiv P(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$.

Очигледно својство симетричног полинома је да су његови коефицијенти уз било која два сабирка облика $x_1^{i_1} \cdots x_n^{i_n}$ и $x_1^{j_1} \cdots x_n^{j_n}$, где је $(j_1, \ldots, j_n)$ пермутација $(i_1, \ldots, i_n)$, једнаки. На пример, ако развој симетричног полинома по x, y, z садржи сабирак x^2y, онда садржи и x^2z, xy^2, итд, са истим коефицијентима.

Примери симетричних полинома су полиноми σ_k $(1 \leq k \leq n)$ уведени у другој глави. Такође је симетричан нпр. полином $x_1^2 + x_2^2$ (по x_1, x_2) који није облика σ_k.

Симетричан полином зовемо *хомогеним* ако су сви његови сабирци истог степена. Еквивалентно, полином T је хомоген степена d ако за свако t и x важи $T(tx_1, \ldots, tx_n) = t^d T(x_1, \ldots, x_n)$. Тако је нпр. $x_1^2 + x_2^2$ хомоген са степеном $n = 2$, али $x_1^2 + x_2^2 + 1$, мада симетричан, није хомоген.

Сваки симетричан полином по $x_1, \ldots, x_n$ се може написати као збир хомогених полинома. Шта више, он је такође представљив у облику линеарне комбинације извесних "цигала". Ове цигле су полиноми

$$T_a = \sum x_1^{a_{i_1}} \cdots x_n^{a_{i_n}} \tag{$*$}$$

за сваку n-торку $a = (a_1, \ldots, a_n)$ ненегативних целих бројева са $a_1 \geq \cdots \geq a_n$, где се сумирање врши по свим пермутацијама $(i_1, \ldots, i_n)$ индекса $1, \ldots, n$. У изразу за T_a исти сабирак може да се понавља више пута, па зато дефинишемо S_a као суму *различитих* сабирака у $(*)$. Полином T_a је увек целобројни умножак S_a. На пример,

$$T_{(2,2,0)} = 2(x_1^2 x_2^2 + x_2^2 x_3^2 + x_3^2 x_1^2) = 2S_{(2,2,0)}.$$

Све n-торке a степена $d = a_1 + \cdots + a_n$ се могу поређати у лексикографски поредак у коме је

$$a > a' \quad \text{ако је} \quad s_1 = s_1', \ldots, s_k = s_k' \text{ и } s_{k+1} > s_{k+1}' \ \text{ за неко } k \geq 1,$$

где је $s_i = a_1 + \cdots + a_i$. У овом поретку најмања n-торка је $m = (x+1, \ldots, x+1, x, \ldots, x)$, где је $x = [d/n]$ и $x+1$ се појављује $d - n[d/n]$ пута.

Полиноми T_a се могу множити по следећој једноставној формули:

T.8.1. Ако су $a = (a_1, \ldots, a_n)$ и $b = (b_1, \ldots, b_n)$ n-торке ненегативних целих бројева, важи

$$T_a \cdot T_b = \sum_{\pi} T_{a+\pi(b)},$$

где се сумира по свим пермутацијама $\pi(b)$ n-торке b. При том је $(x_i)_{i=1}^n + (y_i)_{i=1}^n = (x_i + y_i)_{i=1}^n$.

Доказ. Довољно је приметити да важи

$$x_1^{\pi_1(b)} \cdots x_n^{\pi_n(b)} T_a = \sum x_{i_1}^{a_1 + \pi_{i_1}(b)} \cdots x_{i_n}^{a_n + \pi_{i_n}(b)},$$

а затим сабрати по свим пермутацијама π. $\square$

Наведених цигала има бесконачно много, и оне очигледно нису међусобно независне. Зато нам требају једноставнији градивни елементи који су међусобно независни, а помоћу којих бисмо основним рачунским операцијама могли да изразимо сваки симетричан полином. Испоставља се да су ти атоми управо $\sigma_1, \ldots, \sigma_n$.

- *Пример.* Следећи полиноми по x, y, z су представљиви преко $\sigma_1, \sigma_2, \sigma_3$:

  $xy + yz + zx + x + y + z = \sigma_2 + \sigma_1$;

  $x^2y + x^2z + y^2x + y^2z + z^2x + z^2y = \sigma_1\sigma_2 - 3\sigma_3$;

  $x^2y^2 + y^2z^2 + z^2x^2 = \sigma_2^2 - 2\sigma_1\sigma_3$.

T.8.2. Сваки симетричан полином по $x_1, \ldots, x_n$ се може изразити као полином по $\sigma_1, \sigma_2, \ldots, \sigma_n$. Шта више, симетричан полином са целим коефицијентима је уједно и полином по $\sigma_1, \ldots, \sigma_n$ са целим коефицијентима.

Доказ. Довољно је доказати тврђење за полиноме S_a степена d (за свако d). Користимо индукцију по n-торкама a. Тврђење важи за најмању n-торку m: заиста, $S_m = \sigma_n^q \sigma_r$, где је $d = nq + r$, $0 \leq r < n$. Претпоставимо, дакле, да је тврђење тачно за све полиноме степена мањег од d и за све S_b са $b < a$; докажимо да тада важи и за S_a.

Претпоставимо да је $a = (a_1, \ldots, a_n)$ и да $a_1 = \cdots = a_k > a_{k+1}$ $(k \geq 1)$. Посматрајмо израз $S_a - \sigma_k S_{a'}$, где је $a' = (a_1 - 1, \ldots, a_k - 1, a_{k+1}, \ldots, a_n)$. На основу теореме Т.8.1 лако се види да је тај израз облика $\sum_{b<a} c_b S_b$, где су c_b цели бројеви, те се према индукцијској претпоставци може изразити у облику полинома по σ_i са целим коефицијентима. $\square$

Доказ претходне теореме нам такође даје и алгоритам за представљање сваког симетричног полинома у функцији σ_i. Ипак, за неке специјалне симетричне полиноме постоје и једноставније формуле.

Т.8.3 (Њутнова теорема о симетричним полиномима). Ако означимо $s_k = x_1^k + x_2^k + \cdots + x_n^k$, важи:

$$\begin{array}{rcl} k\sigma_k & = & s_1\sigma_{k-1} - s_2\sigma_{k-2} + \cdots + (-1)^k s_{k-1}\sigma_1 + (-1)^{k+1}s_k; \\ s_m & = & \sigma_1 s_{m-1} - \sigma_2 s_{m-2} + \cdots + (-1)^{n-1}\sigma_n s_{m-n} \quad \text{за } m \geq n. \end{array}$$

(Сви полиноми су по n променљивих.)

Доказ. Директан, нпр. коришћењем формуле Т.8.1. □

Задатак 20. Нека комплексни бројеви $x_1, x_2, \ldots, x_k$ задовољавају

$$x_1^j + x_2^j + \cdots + x_k^j = n, \qquad \text{за } j = 1, 2, \ldots, k,$$

где су n, k дати природни бројеви. Доказати да је

$$(x - x_1)(x - x_2)\ldots(x - x_k) = x^k - \binom{n}{1}x^{k-1} + \binom{n}{2}x^{k-2} - \cdots + (-1)^k\binom{n}{k}.$$

Решење. Дато нам је $s_k = n$ за $k = 1, \ldots, n$. Користећи Њутнову теорему добијамо $\sigma_1 = n$, $\sigma_2 = \frac{1}{2}(n\sigma_1 - n) = \binom{n}{2}$, $\sigma_3 = \frac{1}{3}(n\sigma_2 - n\sigma_1 + n) = \binom{n}{3}$, итд. Доказујемо индукцијом по k да је $\sigma_k = \binom{n}{k}$. Ако је то тачно за $1, \ldots, k-1$, имамо

$$\sigma_k = \frac{n}{k}\left[\binom{n}{k-1} - \binom{n}{k-2} + \binom{n}{k-3} - \cdots\right].$$

Како је $\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1}$, горња једнакост се своди на $\sigma_k = \frac{n}{k}\binom{n-1}{k-1}$, а ово је управо једнако $\binom{n}{k}$.

9° Задаци

1. Монични полином $f(x)$ четвртог степена задовољава $f(1) = 10$, $f(2) = 20$ и $f(3) = 30$. Одредити $f(12) + f(-8)$.

2. Нека су дати комплексни полиноми $P(x) = x^n + a_1x^{n-1} + \cdots + a_n$ са нулама $x_1, \ldots, x_n$, и $Q(x) = x^n + b_1x^{n-1} + \cdots + b_n$ са нулама $x_1^2, \ldots, x_n^2$. Ако су $a_1 + a_3 + a_5 + \cdots$ и $a_2 + a_4 + a_6 + \cdots$ реални бројеви, доказати да је и $b_1 + b_2 + \cdots + b_n$ реалан број.

3. Ако полином P са реалним коефицијентима задовољава за свако x

$$P(\cos x) = P(\sin x),$$

доказати да постоји полином Q такав да је за свако x, $P(x) = Q(x^4 - x^2)$.

4. (a) Доказати да за свако $n \in \mathbb{N}$ постоји полином T_n са целим коефицијентима и водећим коефицијентом 2^{n-1} такав да је $T_n(\cos x) = \cos nx$ за све x.

   (b) Доказати да полиноми T_n задовољавају $T_{m+n} + T_{m-n} = 2T_mT_n$ за све $m, n \in \mathbb{N}$, $m \geq n$.

(c) Доказати да полином U_n дат са $U_n(2x) = 2T_n(x)$ такође има целе коефицијенте, моничан је и задовољава $U_n(x + x^{-1}) = x^n + x^{-n}$.

Полиноми $T_n(x)$ су тзв. *Чебишовљеви* полиноми.

5. Доказати да ако је $\cos\frac{p}{q}\pi = a$ рационалан број за неке $p, q \in \mathbb{Z}$, онда је $a \in \{0, \pm\frac{1}{2}, \pm 1\}$.

6. Доказати да максимум апсолутне вредонсти ма ког реалног моничног полинома n-тог степена на $[-1, 1]$ није мањи од $\frac{1}{2^{n-1}}$.

7. Ако је полином P n-тог степена такав да је $P(i)$ једнако остатку i при дељењу са 2 за $i = 0, 1, \ldots, n$, израчунати $P(n + 1)$.

8. За полином $P(x)$ n-тог степена важи $P(i) = \frac{1}{i}$ за $i = 1, 2, \ldots, n + 1$. Наћи $P(n + 2)$.

9. Ако за реалан полином $P(x)$ важи $P(x) \geq 0$ за свако $x \geq 0$, доказати да постоје реални полиноми $A(x)$ и $B(x)$ такви да је $P(x) = A(x)^2 + xB(x)^2$.

10. Доказати да се полином $P(x, y) = x^4y^2 + x^2y^4 - 3x^2y^2 + 1$, иако је ненегативан за све $x, y \in \mathbb{R}$, не може написати у облику збира квадрата неколико полинома.

11. Нека су $f(x), g(x)$ и $a(x, y)$ полиноми са реалним коефицијентима такви да је $f(x) - f(y) = a(x, y)(g(x) - g(y))$ за све реалне x, y. Доказати да постоји полином h такав да је $f(x) = h(g(x))$ за све $x \in \mathbb{R}$.

12. Ако једначина $Q(x) = ax^2 + (c - b)x + (e - d) = 0$ има реалне корене веће од 1, где су $a, b, c, d, e \in \mathbb{R}$, доказати да једначина $P(x) = ax^4 + bx^3 + cx^2 + dx + e = 0$ има бар један реалан корен.

13. Моничан полином P са реалним коефицијентима задовољава $|P(i)| < 1$. Доказати да постоји корен $z = a + bi$ такав да је $(a^2 + b^2 + 1)^2 < 4b^2 + 1$.

14. Дати су неконстантни полиноми $P(x) = x^m + \cdots + a_1x + a_0$ и $Q(x) = x^n + \cdots + b_1x + b_0$. Доказати да збир квадрата коефицијената полинома $P(x)Q(x)$ није мањи од $a_0^2 + b_0^2$.

15. За које реалне вредности a постоји рационална функција $f(x)$ која задовољава $f(x^2) = f(x)^2 - a$? (Рационална функција је количник два полинома.)

16. Наћи све полиноме P који задовољавају $P(x^2 + 1) = P(x)^2 + 1$ за све x.

17. Наћи све полиноме P за које је $P(x)^2 - 2 = 2P(2x^2 - 1)$.

18. Ако полиноми P и Q имају бар по један реалан корен, и
$$P(1 + x + Q(x)^2) = Q(1 + x + P(x)^2),$$
доказати да је $P \equiv Q$.

19. Наћи све полиноме $P(x)$ са реалним коефицијентима који задовољавају једнакост
$$P(a - b) + P(b - c) + P(c - a) = 2P(a + b + c)$$
за све тројке (a, b, c) реалних бројева таквих да је $ab + bc + ca = 0$. *(ММО 2004.2)*

20. Низ целих бројева $(a_n)_{n=1}^{\infty}$ има својство да $m-n \mid a_m - a_n$ за све различите $m, n \in \mathbb{N}$. Претпоставимо да постоји полином $P(x)$ такав да је $|a_n| < P(n)$ за све n. Доказати да постоји полином $Q(x)$ такав да је $a_n = Q(n)$ за све n.

21. Нека је $P(x)$ полином степена $n > 1$ са целим коефицијентима и нека је k природан број. Посматрајмо полином $Q(x) = P(P(\ldots P(P(x))\ldots))$, где се P појављује k пута. Доказати да постоји највише n целих бројева t таквих да је $Q(t) = t$. *(ММО 2006.5)*

22. Ако су P и Q монични полиноми такви да је $P(P(x)) = Q(Q(x))$, доказати да је $P \equiv Q$.

23. Нека су m, n и a природни бројеви и $p < a-1$ прост. Доказати да је полином $f(x) = x^m(x-a)^n + p$ нерастављив.

24. Доказати да је полином $F(x) = (x^2+x)^{2^n} + 1$ нерастављив за све $n \in \mathbb{N}$.

25. Полином $P(x)$ има особину да за свако $y \in \mathbb{Q}$ постоји $x \in \mathbb{Q}$ такво да је $P(x) = y$. Доказати да је P линеаран полином.

26. Нека је k природан број. Претпоставимо да постоји низ целих бројева $a_0, a_1, \ldots$ такав да је

$$a_n = \frac{a_{n-1} + n^k}{n} \quad \text{за све } n \geq 1.$$

Доказати да је $k-2$ дељиво са 3.

27. Нека је $P(x)$ монични полином степена n чије су нуле $i-1, i-2, \ldots, i-n$ (где је $i^2 = -1$) и нека су $R(x)$ и $S(x)$ реални полиноми такви да је $P(x) = R(x) + iS(x)$. Доказати да полином $R(x)$ има n реалних нула.

28. Претпоставимо да моничан полином $P(x)$ са целобројним коефицијентима има све нуле по модулу једнаке 1. Доказати прво да таквих полинома датог степена има само коначно много, а онда извести да су све његове нуле корени јединице, тј. да $P(x) \mid (x^n - 1)^k$ за неке природне n, k.

10° **Решења**

1. Полином $f(x) - 10x$ се анулира у тачкама $x = 1, 2, 3$, па је дељив полиномом $(x-1)(x-2)(x-3)$. Из моничности следи да је $f(x) - 10x = (x-1)(x-2)(x-3)(x-c)$ за неко c. Сада је

$$f(12) + f(-8) = 11 \cdot 10 \cdot 9 \cdot (12-c) + 120 + (-9)(-10)(-11)(-8-c) - 80 = 19840.$$

2. Приметимо да је $Q(x^2) = \prod(x^2 - x_i^2) = \prod(x - x_i) \cdot \prod(x + x_i) = (-1)^n P(x)P(-x)$. Сада имамо

$$b_1 + b_2 + \cdots + b_n = Q(1) - 1 = (-1)^n P(1)P(-1) - 1 = (-1)^n(1 + B - A)(1 + B + A),$$

где су $A = a_1 + a_3 + a_5 + \cdots$ и $B = a_2 + a_4 + \cdots$.

3. Из услова следи да је $P(-\sin x) = P(\sin x)$, тј. $P(-t) = P(t)$ за бесконачно много t, па полиноми $P(x)$ и $P(-x)$ морају да се поклапају. Дакле, $P(x) = S(x^2)$ за неки полином S. Сада је $S(\cos^2 x) = S(\sin^2 x)$ за свако x, тј. $S(1-t) = S(t)$ за бесконачно много вредности t, што даје $S(x) \equiv S(1-x)$. То је еквивалентно са $R(x-\frac{1}{2}) = R(\frac{1}{2}-x)$, тј. $R(y) \equiv R(-y)$, где је R полином такав да је $S(x) = R(x-\frac{1}{2})$. Сада је $R(x) = T(x^2)$ за неки полином T, и најзад $P(x) = S(x^2) = R(x^2-\frac{1}{2}) = T(x^4-x^2+\frac{1}{4}) = Q(x^4-x^2)$ за неки полином Q.

4. (a) Очигледно $T_0(x) = 1$ и $T_1(x) = x$ задовољавају услове. За $n > 1$ користимо индукцију по n. Како је $\cos(n+1)x = 2\cos x \cos nx - \cos(n-1)x$, можемо узети $T_{n+1} = 2T_1T_n - T_{n-1}$. Како су T_1T_n и T_{n-1} редом степена $n+1$ и $n-1$, T_{n+1} је степена $n+1$ и има водећи коефицијент $2\cdot 2^n = 2^{n+1}$. Из конструкције следи и да су му сви коефицијенти цели.

   (b) Једнакост следи из идентитета $\cos(m+n)x + \cos(m-n)x = 2\cos mx \cos nx$.

   (c) Низ полинома (U_n) задовољава $U_0(x) = 2$, $U_1(x) = x$ и $U_{n+1} = U_1U_n - U_{n-1}$, одакле индукцијом следи моничност и целобројност коефицијената. Једнакост $U_n(x+x^{-1}) = x^n + x^{-n}$ важи за свако $x = \cos t + i\sin t$, па према томе важи за све x.

5. Претпоставимо да важи $\cos\frac{p}{q}\pi = a$. Према претходном задатку је $U_q(2a) = 2\cos p\pi = \pm 2$, при чему је U_q моничан и са целим коефицијентима, па је $2a$ цео на основу теореме 3.2.

6. Приметимо да једнакост важи за умножак n-тог Чебишовљевог полинома $T_n(x)$. Водећи коефицијент T_n је 2^{n-1}, па је $C_n(x) = \frac{1}{2^{n-1}}T_n(x)$ моничан полином и
$$|T_n(x)| = \frac{1}{2^{n-1}}\,|\cos(n\arccos x)| \le \frac{1}{2^{n-1}} \quad \text{за } x \in [-1,1].$$
Шта више, T_n у тачкама $1, \cos\frac{\pi}{n}, \cos\frac{2\pi}{n}, \cdots, \cos\frac{(n-1)\pi}{n}, -1$ наизменично узима вредности $\frac{1}{2^{n-1}}$ и $-\frac{1}{2^{n-1}}$.

   Претпоставимо да је $P \neq T_n$ моничан полином такав да је $\max_{-1\le x\le 1}|P(x)| < \frac{1}{2^{n-1}}$. Тада је $P(x) - C_n(x)$ у тачкама $1, \cos\frac{\pi}{n}, \cdots, \cos\frac{(n-1)\pi}{n}, -1$ наизменично позитивно и негативно, тако да полином $P - C_n$ има бар n нула, по једну на сваком интервалу између две суседне тачке. Међутим, $P - C_n$ је полином степена $n-1$ јер се моном x^n потире, па је то немогуће.

7. Како је $P^{[i]}(x) = (-2)^{i-1}(-1)^x$ за $x = 0, 1, \dots, n-i$, имамо
$$P(n+1) = P(n) + P^{[1]}(n-1) + \cdots + P^{[n]}(0) = \begin{cases} 2^n, & 2 \nmid n; \\ 1-2^n, & 2 \mid n. \end{cases}$$

8. По теореми 5.2 имамо
$$P(n+2) = \sum_{i=0}^{n}(-1)^{n-i}\frac{1}{i+1}\binom{n+1}{i} = \frac{1}{n+2}\sum_{i=0}^{n}(-1)^{n-i}\binom{n+2}{i+1} = \begin{cases} 0, & 2 \nmid n; \\ \frac{2}{n+2}, & 2 \mid n. \end{cases}$$

9. По теореми Т.1.9, полином $P(x)$ се може представити у облику
$$P(x) = (x-a_1)^{\alpha_1}\cdots(x-a_k)^{\alpha_k}\cdot(x^2-b_1x+c_1)\cdots(x^2-b_mx+c_m), \qquad (*)$$
при чему су a_i, b_j, c_j реални бројеви такви да су a_i различити и полиноми $x^2 - b_ix + c_i$ немају реалних нула.

Из услова $P(x) \geq 0$ за све $x \geq 0$ следи да је $(\forall i)$ α_i парно или $a_i < 0$. Сада је лако представити сваки од чинилаца у $(*)$ у облику $A^2 + xB^2$, па је по познатој формули $(a^2+\gamma b^2)(c^2+\gamma d^2) = (ac+\gamma bd)^2+\gamma(ad-bc)^2$ њихов производ $P(x)$ такође могуће представити у жељеном облику.

10. Претпоставимо супротно, да постоје полиноми $Q_1, \dots, Q_n$ по x и y такви да је $Q_1(x,y)^2 + \cdots + Q_n(x,y)^2 = P(x,y)$. Тада је $\sum_i Q_i(x,0)^2 = 1$, па следи да полиноми $Q_i(x,0) = c_i$ морају бити константни по x. То значи да је полином $Q_i(x,y) - c_i$ дељив са y. Аналогно, дељив је и са x, па закључујемо да је $Q_i(x,y) = c_i + xyR_i(x,y)$ за неки полином R_i. Како је $\deg Q_i \leq 3$, полиноми R_i морају бити линеарни. Сада имамо $\sum_{i=1}^n (c_i + xyR_i)^2 = \sum_{i=1}^n (c_i^2 + 2c_ixyR_i + x^2y^2R_i^2) = x^2y^2(x^2+y^2-3)+1$, тј.

$$x^2y^2\left(x^2+y^2-3-\sum_{i=1}^n R_i^2\right) = \sum_{i=1}^n (c_i^2 + 2c_ixyR_i) - 1.$$

Међутим, на левој страни ове једнакости је полином дељив са x^2y^2 (степена 4), а на десној је полином степена највише 3. То је могуће једино ако је са обе стране 0, али то води у контрадикцију јер полином са леве стране очигледно узима негативну вредност за нпр. $x = y = 1$.

11. Означимо $\deg f = n$ и $\deg g = m$. Тврђење доказујемо индукцијом по n. Ако је $n < m$, онда је $\deg_x[f(x) - f(y)] < \deg_x[g(x) - g(y)]$, одакле је $f(x) - f(y) = 0$, тј. f је константно, па тврђење тривијално важи.

    Нека је $n \geq m$. Преласком на $f_1(x) = f(x) - f(0)$ и $g_1(x) = g(x) - g(0)$ по потреби, можемо да претпоставимо да је $f(0) = g(0) = 0$. Услов задатка за $y = 0$ даје $f(x) = A(x)g(x)$, где је $A(x) = a(x,0)$ и $\deg A = n - m$. Сада имамо

$$\begin{aligned} a(x,y)(g(x)-g(y)) &= f(x) - f(y) = A(x)g(x) - A(y)g(y) \\ &= [A(x)-A(y)]g(x) + A(y)[g(x)-g(y)]. \end{aligned}$$

    Одавде је полином $[A(x)-A(y)]g(x)$ дељив са $g(x)-g(y)$, дакле $A(x)-A(y) = b(x,y)(g(x)-g(y))$ за неки полином $b(x,y)$. По индукцијској претпоставци, постоји полином h_1 такав да је $A(x) = h_1(g(x))$, и одатле $f(x) = g(x)\cdot h_1(g(x)) = h(g(x))$ за $h(t) = th_1(t)$. Овим је индукција готова.

12. Напишимо

$$P(-x) = ax^4 + (c-b)x^2 + (e-d) - b(x^3 - x^2) - d(x-1).$$

    Ако је r нула полинома Q, имамо $P(\sqrt{r}) = -(\sqrt{r}-1)(br+d)$ и $P(-\sqrt{r}) = (\sqrt{r}+1)(br+d)$. Видимо да је један од бројева $P(\pm\sqrt{r})$ позитиван а други негативан (или су оба 0), па негде између $-\sqrt{r}$ и $\sqrt{r}$ мора постојати нула полинома P јер је $\sqrt{r} > 1$.

13. Нека је $P(x) = (x-x_1)\cdots(x-x_m)(x^2-p_1x+q_1)\cdots(x^2-p_nx+q_n)$, при чему полиноми $x^2 - p_kx + q_k$ немају реалних нула. Имамо

$$1 > |P(i)| = \prod_{j=1}^m |i - x_j| \prod_{k=1}^n |-1-p_ki+q_k|,$$

    а како је $|i-x_j|^2 = 1+x_j^2 > 1$ за све j, за неко k мора да важи $|-1-p_ki+q_k| < 1$, тј.

$$p_k^2 + (q_k-1)^2 < 1. \qquad (*)$$

Нека су $a \pm bi$ корени полинома $x^2 - p_k x + q_k$ (они су такође корени полинома P). Тада је $p_k = 2a$ и $q_k = a^2 + b^2$, па неједнакост $(*)$ постаје $4a^2 + (a^2 + b^2 - 1)^2 < 1$, што је еквивалентно жељеној неједнакости.

14. Означимо $a_m = b_n = 1$. Нека је $P(x)Q(x) = c_{m+n}x^{m+n} + \cdots + c_1 x + c_0$ и $P(x)Q(1/x) = d_m x^m + \cdots + d_{-n}x^{-n}$.

    Доказаћемо да важи $\sum_i c_i^2 = \sum_j d_j^2$. Тражена неједнакост ће одмах следити одавде јер је $d_m = b_0$ и $d_{-n} = a_0$.

    Коефицијент c_k је једнак суми $\sum_{i+j=k} a_i b_j$, што даје $c_k^2 = \sum_{i+j=r+s=k} a_i a_r b_j b_s$, па имамо $\sum_k c_k^2 = \sum_{i+j=r+s} a_i a_r b_j b_s$. С друге стране, коефицијент d_k је једнак $\sum_{t-u=k} a_t b_u$, што даје $d_k^2 = \sum_{t-u=v-w=k} a_t a_v b_u b_w$, а тада је

$$\sum_k d_k^2 = \sum_{t-u=v-w} a_t a_v b_u b_w = \sum_{t+w=u+v} a_t a_v b_u b_w = \sum_k c_k^2,$$

    што смо и тврдили.

15. Напишимо f у облику $f = P/Q$, где су P и Q узајамно прости полиноми и Q је моничан. Услов задатка постаје $P(x^2)/Q(x^2) = P(x)^2/Q(x)^2 - a$. Упоређивањем водећег коефицијента закључујемо да је и P моничан. Како су и $P(x^2)$ и $Q(x^2)$ узајамно прости (ако они имају заједничку нулу, имају је и P и Q), следи $Q(x^2) = Q(x)^2$. Одавде је $Q(x) = x^n$ за неко $n \in \mathbb{N}$. Сада имамо $P(x^2) = P(x)^2 - ax^{2n}$.

    Нека је $P(x) = a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} + x^m$. Упоређивањем коефицијената $P(x)^2$ и $P(x^2)$ видимо да је $a_{n-1} = \cdots = a_{2m-n+1} = 0$, $a_{2m-n} = a/2$, $a_1 = \cdots = a_{m-1} = 0$ и $a_0 = 1$. Одавде закључујемо да је или $a = 0$, или $a = 2$ и $2m - n = 0$.

16. Како је P симетричан у односу на тачку 0, није тешко показати да је P уједно полином по x^2, тако да постоји полином Q такав да је $P(x) = Q(x^2+1)$ или $P(x) = xQ(x^2+1)$. Тада је $Q((x^2+1)^2+1) = Q(x^2+1)^2 - 1$, односно $(x^2+1)Q((x^2+1)^2+1) = x^2Q(x^2+1)^2 + 1$. Смена $x^2+1 = y$ даје $Q(y^2+1) = Q(y)^2+1$, односно $yQ(y^2+1) = (y-1)Q(y)^2+1$.

    Претпоставимо да је $yQ(y^2+1) = (y-1)Q(y)^2+1$. Убацивањем $y = 1$ добијамо $Q(2) = 1$. Приметимо да, ако је $a \neq 0$ и $Q(a) = 1$, онда је $aQ(a^2+1) = (a-1)+1$ па је и $Q(a^2+1) = 1$. Овако добијамо бесконачан низ (a_n) тачака у којима Q узима вредност 1, дат са $a_0 = 2$ и $a_{n+1} = a_n^2 + 1$. Закључујемо да је $Q \equiv 1$.

    Показали смо да ако је $Q \not\equiv 1$, онда је $P(x) = Q(x^2+1)$. Сада лако долазимо до свих решења: то су полиноми облика $T(T(\cdots(T(x))\cdots))$, где је $T(x) = x^2+1$.

17. Означимо $P(1) = a$. Имамо $a^2 - 2a - 2 = 0$. Како је $P(x) = (x-1)P_1(x) + a$, убацивањем у полазну једначину и срећивањем добијамо $(x-1)P_1(x)^2 + 2aP_1(x) = 4(x+1)P_1(2x^2-1)$. За $x = 1$ имамо $2aP_1(1) = 8P_1(1)$, па због $a \neq 4$ следи $P_1(1) = 0$, тј. $P_1(x) = (x-1)P_2(x)$, тј. $P(x) = (x-1)^2P_2(x) + a$. Претпоставимо да је $P(x) = (x-1)^nQ(x) + a$, при чему је $Q(1) \neq 0$. Убацивањем у полазну релацију и срећивањем добијамо $(x-1)^nQ(x)^2 + 2aQ(x) = 2(2x+2)^nQ(2x^2-1)$, што опет даје $Q(1) = 0$, контрадикција. Закључујемо да је $P(x) = a$.

18. Приметимо да постоји $x = a$такво да је $P(a)^2 = Q(a)^2$. Ово следи из чињенице да, ако су p и q редом реални коренови P и Q, онда је $P(p)^2 - Q(p)^2 \leq 0 \leq P(q)^2 - Q(q)^2$, а $P^2 - Q^2$ је непрекидна функција. Сада је $P(b) = Q(b)$ за $b = 1 + a + P(a)^2$. Ако претпоставимо да је a највећи реалан број такав да је $P(a) = Q(a)$, одмах долазимо до контрадикције.

19. Нека је $P(x) = a_0 + a_1x + \cdots + a_nx^n$. За свако x тројка $(a, b, c) = (6x, 3x, -2x)$ задовољава услов $ab + bc + ca = 0$. Услов по P нам даје $P(3x) + P(5x) + P(-8x) = 2P(7x)$ за све x, одакле упоређивањем коефицијената добијамо $K(i) = \left(3^i + 5^i + (-8)^i - 2 \cdot 7^i\right) = 0$ кад год је $a_i \neq 0$. Како је $K(i)$ негативно за непарно i и позитивно за $i = 0$ и парно $i \geq 6$, $a_i = 0$ је могуће само за $i = 2$ и $i = 4$. Према томе, $P(x) = a_2x^2 + a_4x^4$ за неке реалне бројеве a_2, a_4. Лако се проверава да сви овакви $P(x)$ задовољавају тражени услов.

20. Нека је P степена d. Постоји јединствен полином Q степена не већег од d такав да је $Q(k) = a_k$ за $k = 1, 2, \ldots, d+1$. Докажимо да је $Q(n) = a_n$ за све n.

    Нека је $n > d+1$. Полином Q можда нема целе коефицијенте, па не можемо да закључимо да $n - m \mid Q(n) - Q(m)$, али знамо да има рационалне, тј. постоји природан број M такав да $R(x) = MQ(x)$ има целе коефицијенте. По услову задатка, $M(a_n - Q(n)) = M(a_n - a_k) - (R(n) - R(k))$ је дељиво са $n - k$ за свако $k = 1, 2, \ldots, d + 1$. Према томе, за свако n важи или $a_n = Q(n)$, или

$$L_n = \operatorname{lcm}(n-1, n-2, \ldots, n-d-1) \leq M(a_n - Q(n)) < Cn^d$$

    за неку константу C која не зависи од n.

    Претпоставимо да $a_n \neq Q(n)$ за неко n. Приметимо да L_n није мање од производа $(n-1)\cdots(n-d-1)$ подељеног производом P свих $\gcd(n-i, n-j)$ по свим паровима (i, j) различитих бројева из $\{1, 2, \ldots, d+1\}$. При том је $\gcd(n-i, n-j) \leq i - j$, тако да је $P \leq 1^d 2^{d-1} \cdots d$. Следи да је

$$(n-1)(n-2)\cdots(n-d-1) \leq PL_n < CPn^d,$$

    што није тачно за довољно велико n јер је лева страна полином степена $d+1$. Дакле, $a_n = Q(n)$ за свако довољно велико n, рецимо $n > N$.

    Шта се догађа за $n \leq N$? По услову задатка, $M(a_n - Q(n)) = M(a_n - a_k) - (R(n) - R(k))$ је дељиво са $m - n$ за свако $m > N$, па отуд мора бити једнако нули. Дакле, $a_n = Q(n)$ за све n.

21. У задатку 6 из текста је доказано да свако такво t такође задовољава $P(P(t)) = t$. Ако свако такво t задовољава $P(t) = t$, број решења не прелази $\deg P = n$. Претпоставимо да је $P(t_1) = t_2$, $P(t_2) = t_1$, $P(t_3) = t_4$ и $P(t_4) = t_3$, при чему је $t_1 \neq t_{2,3,4}$. По теореми 2.1, $t_1 - t_3$ дели $t_2 - t_4$ и обрнуто, одакле следи $t_1 - t_3 = \pm(t_2 - t_4)$. Претпоставимо да је $t_1 - t_3 = t_2 - t_4$, тј. $t_1 - t_2 = t_3 - t_4 = k \neq 0$. Како на сличан начин важи $t_1 - t_4 = \pm(t_2 - t_3)$, добијамо $t_1 - t_3 + k = \pm(t_1 - t_3 - k)$ што је немогуће. Према томе, мора да важи $t_1 - t_3 = t_4 - t_2$, из чега закључујемо $P(t_1) + t_1 = P(t_3) + t_3 = c$ за неко c. Следи да сва целобројна решења t једначине $P(P(t)) = t$ задовољавају $P(t) + t = c$, те њихов број не прелази n.

22. Претпоставимо да је $R = P - Q \neq 0$ и да је $0 < k \leq n - 1$ степен $R(x)$. Тада је

$$P(P(x)) - Q(Q(x)) = [Q(P(x)) - Q(Q(x))] + R(P(x)).$$

    Ако напишемо $Q(x) = x^n + \cdots + a_1x + a_0$, имамо

$$Q(P(x)) - Q(Q(x)) = [P(x)^n - Q(x)^n] + \cdots + a_1[P(x) - Q(x)],$$

    при чему сви сабирци осим првог имају степен највише $n^2 - n$, док је први сабирак једнак $R(x) \cdot \left(P(x)^{n-1} + P(x)^{n-2}Q(x) + \cdots + Q(x)^{n-1}\right)$ и отуда има степен $n^2 - n + k$ са водећим коефицијентом n. Дакле, степен $Q(P(x)) - Q(Q(x))$ је $n^2 - n + k$. Степен полинома $R(P(x))$ је једнак $kn < n^2 - n + k$, одакле закључујемо да је разлика $P(P(x)) - Q(Q(x))$ степена $n^2 - n + k$, што је контрадикција.

Остаје случај када је $R \equiv c$ константно. Тада услов $P(P(x)) = Q(Q(x))$ даје $Q(Q(x)+c) = Q(Q(x)) - c$, па једнакост $Q(y+c) = Q(y) - c$ важи за бесконачно много y, одакле је $Q(y+c) \equiv Q(y) - c$ што је могуће само за $c = 0$ (довољно је упоредити коефицијенте).

23. Претпоставимо да је $f(x) = g(x)h(x)$ за неке неконстантне полиноме са целим коефицијентима. Пошто је $|f(0)| = p$, важи или $|g(0)| = 1$ или $|h(0)| = 1$. Претпоставимо без смањења општости да је $|g(0)| = 1$. Због $|g(a)h(a)| = p$ је $|g(a)| \in \{1, p\}$, а осим тога a дели $|g(a) - g(0)| \leq p + 1 < a$, па мора да буде $g(a) = g(0) = 1$. С друге стране, нека је $g(x) = (x - \alpha_1) \cdots (x - \alpha_k)$. Тада је $|\alpha_1 \cdots \alpha_k| = 1$. Како је $f(\alpha_i) - p = \alpha_i^m (\alpha_i - a)^n = -p$, узимајући производ по $i = 1, 2, \ldots, k$ добијамо $1 = |g(a)|^n = |(\alpha_1 - a) \cdots (\alpha_k - a)|^n = p^k$, што је немогуће.

24. Претпоставимо да је $F = G \cdot H$ за неке полиноме G, H са целим коефицијентима. Сведимо ову једнакост по модулу 2. Како је $(x^2+x+1)^{2^n} \equiv F(x) \pmod 2$, добијамо $(x^2+x+1)^{2^n} = g(x)h(x)$, где су $g \equiv G$ и $h \equiv H$ полиноми над $\mathbb{Z}_2$. Полином $x^2 + x + 1$ је нерастављив над $\mathbb{Z}_2[x]$, па постоји природан број k такав да је $g(x) = (x^2+x+1)^k$ и $h(x) = (x^2+x+1)^{2^n-k}$; овде се наравно мисли на једнакости у $\mathbb{Z}_2[x]$.

Назад у $\mathbb{Z}[x]$, овај услов постаје $H(x) = (x^2+x+1)^{2^n-k} + 2V(x)$ и $G(x) = (x^2+x+1)^k + 2U(x)$ за неке полиноме U и V са целим коефицијентима. Дакле,

$$[(x^2+x+1)^k + 2U(x)][(x^2+x+1)^{2^n-k} + 2V(x)] = F(x).$$

Ако сада заменимо $x = \epsilon = \frac{-1+i\sqrt{3}}{2}$ у последњу једнакост, добијамо $U(\epsilon)V(\epsilon) = \frac{1}{4}F(\epsilon) = \frac{1}{2}$. Међутим, ово је немогуће јер полином $U(x)V(x)$ има целе коефицијенте, те $U(\epsilon)V(\epsilon)$ мора бити облика $a + b\epsilon$ за неке $a, b \in \mathbb{Z}$ (јер је $\epsilon^2 = -1 - \epsilon$), а $\frac{1}{2}$ то није.

25. Јасно је, на пример из теореме 4.1, да P мора да има рационалне коефицијенте. За неко $m \in \mathbb{N}$ коефицијенти полинома $mP(x)$ су цели. Нека је p прост број који не дели m. Тврдимо да, ако P није линеарно, не постоји рационалан број x такав да је $P(x) = \frac{1}{mp}$. Наиме, ако би такво x постојало, важило би и $Q(x) = mpP(x) - 1 = 0$. Међутим, $Q(x)$ је нерастављив јер је по Ајзенштајновом критеријуму то и $x^n Q(1/x)$ будући да су му сви коефицијенти осим првог дељиви са p и слободни члан није дељив са p^2.

26. Показаћемо да мора да постоји полином $P(x)$ такав да је $a_n = P(n)$.

За почетак, приметимо да за свако $k \in \mathbb{N}$ постоје полином P_k степена $k-1$ са целобројним коефицијентима и цео број q_k такав да је

$$P_k(x) = \frac{x^k + P_k(x-1) + q_k}{x}. \qquad (*_k)$$

Наиме, ако за дато k напишемо $P_k(x) = b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$, упоређивањем коефицијената уз x_i $(i = k-1, \ldots, 0)$ у xP_k и $x^k + P_k(x-1) + q_k$ можемо да једнозначно одредимо $b_{k-1}, \ldots, b_0$ редом и $q_k = -P_k(-1)$.

Из рекурентних релација за $P_k(x)$ и низ a_n следи индукцијом

$$a_n - P_k(n) = \frac{a_{n-1} - P_k(n-1)}{n} - \frac{q_k}{n} = \cdots = \frac{a_0 - P_k(0)}{n!} - q_k \sum_{i=0}^{n-1} \frac{i!}{n!} \quad \text{за све } n \geq 1.$$

Како је у претходној једнакости лева страна цео број, а десна тежи нули, мора бити $a_n = P_k(n)$ за све n и $q_k = 0$.

Сада из релација $(*_k)$, $(*_{k+1})$ и $(*_{k+2})$ добијамо релацију $(x^2+x)(*_k)-(*_{k+1})-(*_{k+2})$ која након сређивања постаје

$$xT_k(x)-T_k(x-1) = 2x(P_k(x-1)+q_k)-(q_k+q_{k+1}+q_{k+2}) \equiv q_k+q_{k+1}+q_{k+2} \pmod 2,$$

где је $T_k(x) = (x^2+x)P_k(x) - P_{k+1}(x) - P_{k+2}(x) - q_k x$.

Упоређивањем степена одмах видимо да је ово могуће само кад је $T_k \equiv 0$ по модулу 2 и $q_{k+2} \equiv q_{k+1} + q_k \pmod 2$. Како је $q_1 = -1$ и $q_2 = 0$, q_k је парно само за $k \equiv 2 \pmod 3$ одакле следи тврђење.

27. Означимо $P(x) = P_n(x) = R_n(x) + iS_n(x)$. Доказаћемо индукцијом по n да су све нуле P_n реалне; шта више, ако су $x_1 > x_2 > \cdots > x_n$ нуле R_n и $y_1 > y_2 > \cdots > y_{n-1}$ нуле R_{n-1}, да тада важи

$$x_1 > y_1 > x_2 > y_2 > \cdots > x_{n-1} > y_{n-1} > x_n.$$

Ово тврђење је тривијално тачно за $n = 1$. Претпоставимо да важи за $n-1$.

Како је $R_n + iS_n = (x-i+n)(R_{n-1}+iS_{n-1})$, полиноми R_n и S_n су рекурентно повезани релацијама $R_n = (x+n)R_{n-1}+S_{n-1}$ и $S_n = (x+n)S_{n-1}-R_{n-1}$. Одавде добијамо

$$R_n - (2x+2n-1)R_{n-1} + [(x+n-1)^2+1]R_{n-2} = 0.$$

Ако су $z_1 > \cdots > z_{n-2}$ (реалне) нуле R_{n-2}, по индуктивној претпоставци имамо $z_{i-1} > y_i > z_i$; како је вредност полинома R_{n-2} наизменично позитивна и негативна на интервалима $(z_1, +\infty)$, (z_2, z_1), итд, следи да је $\operatorname{sgn} R_{n-2}(y_i) = (-1)^{i-1}$. Сада из релације $R_n(y_i) = -[(x+n-1)^2+1]R_{n-2}(y_i)$ закључујемо да је

$$\operatorname{sgn} R_n(y_i) = (-1)^i,$$

што значи да полином R_n има нулу на сваком од n интервала $(y_1, +\infty)$, (y_2, y_1), ..., $(-\infty, y_{n-1})$. Индукција је готова.

28. Фиксирајмо $\deg P = n$. Нека је $P(x) = (x-z_1)\cdots(x-z_n) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, где је $|z_i| = 1$ за $i = 1, \ldots, n$. По Вијетовим формулама је $a_{n-i} = \pm\sigma_i(z_1, \ldots, z_n)$ што је збир $\binom{n}{i}$ сабирака модула 1, одакле следи да је $|a_{n-i}| \le \binom{n}{i}$. Према томе, постоји највише $2\binom{m}{i}+1$ могућих вредности коефицијента $P(x)$ уз x^{n-i} за свако i, одакле следи да је и број могућих полинома P степена n коначан.

Сада посматрајмо полином $P_r(x) = (x-z_1^r)\cdots(x-z_n^r)$ за сваки природан број r. Сви коефицијенти полинома P_r су симетрични полиноми по z_i са целим коефицијентима, па по теореми Т.8.2 сви они морају бити цели. Према томе, сваки полином P_r задовољава услове задатка, али r-ова је бесконачно много, а таквих полинома коначно много. Према томе, $P_r(x) = P_s(x)$ за неке различите $r, s \in \mathbb{N}$, одакле следи тврђење.