Универзитет у Београду

Математички факултет

МАСТЕР РАД

КРИТЕРИЈУМИ НЕРАСТАВЉИВОСТИ ПОЛИНОМА НАД ПРСТЕНОМ ЦЕЛИХ БРОЈЕВА

СТУДЕНТ

Душан Радојевић

МЕНТОР

Марко Радовановић

Београд, 2023.

Садржај

1. Увод

У уводном делу рада увешћемо основне појмове и дати преглед неких класичних тврђења, као што је својство једнозначне факторизације за прстен полинома са целобројним коефицијентима и Гаусова лема.

У наставку разматраћемо критеријуме нерастављивости у овом прстену. Њих ћемо поделити у три групе. Прво ћемо дати критеријуме засноване на аритметичким особинама коефицијената; даћемо Ајзенштајнов критеријум, као и нека његова уопштења. Између осталог, биће приказано како се Њутнов дијаграм може применити за испитивање нерастављивости. Затим ћемо дати критеријуме нерастављивости за полиноме који имају 'доминантан' коефицијент, а на крају и критеријуме који комбинују претходне две особине.

У завршном делу рада, кроз неколико задатака, приказаћемо и друге идеје које могу бити од користи приликом испитивања нерастављивости полинома.

2. Дефиниције и општа својства полинома

2.1. Прстен полинома

У овом одељку даћемо преглед најважнијих дефиниција и теорема о полиномима, које ће бити пропраћене примерима.

Пре него што дефинишемо појам полинома над прстеном, присетимо се најпре дефиниције прстена.

Дефиниција 2.1. Уређена тројка $(\mathcal{Z}, +, \cdot)$, где је $\mathcal{Z}$ непразан скуп, је прстен ако важи:

1) $(\mathcal{Z}, +)$ је комутативна група;
2) $(\mathcal{Z}, \cdot)$ је полугрупа;
3) за све $a, b, c \in \mathcal{Z}$ важи $a \cdot (b + c) = a \cdot b + a \cdot c$ и $(b + c) \cdot a = b \cdot a + c \cdot a$.

Дакле, скуп $\mathcal{Z}$ је такав да је у њему бинарна операција + асоцијативна и комутативна, постоји неутрал 0 у односу на сабирање и за сваки елемент из тог скупа постоји њему супротан елемент из прстена тако да је њихов збир једнак нули.

Пример 2.1. Уређену тројку $(\mathbb{Z}, +, \cdot)$ називамо прстен целих бројева. Специјално у овом случају важи да је операција $\cdot$ комутативна, па такав прстен називамо *комутативни прстен*.

Након дефинисања прстена и основних својстава операција које важе у њему, уведимо сада појам полинома и објаснимо његова општа својсва.

Дефиниција 2.2. Полином по променљивој x над прстеном $\mathcal{Z}$ је израз облика

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

где елементе $a_n, \ldots, a_0$ из скупа $\mathcal{Z}$ називамо коефицијентима полинома, а број n степеном полинома, уколико важи $a_n \neq 0$. Полином којем су сви коефицијенти једнаки нули назива се нула-полином.

Ова дефиниција је уопштена, а у зависности ком скупу коефицијенти припадају (прстену целих, пољу рационалних, реалних или комплексних бројева), скупове полинома означићемо са $\mathbb{Z}[x]$, односно, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$.

Дефиниција 2.3. Израз облика cx^k, где је k ненегативан цео број, а c елемент скупа $\mathcal{Z}$ назива се моном, збир два монома називамо бином, три монома трином, те ће и уопштено сваки збир неколико монома бити полином, што нам говори и дефиниција 2.2.

Пример 2.2. Полином $x^2 + x + 1$ представља полином другог степена са целобројним коефицијентима. Како је он збир три монома, он је уједно и трином.

Дефиниција 2.4. У зависности од степена полинома, тј. да ли је полином првог, другог или трећег степена, разликоваћемо *линеарне*, *квадратне* и *кубне* полиноме.

У запису полинома може се јавити више различитих променљивих, па се користе неки од следећих записа: $p(x) = x^2 + x + 1$. Ово је, заправо, запис полинома p, где је наглашено да се само променљива x налази у његовом запису. Слично тако, $q(x, y) = x^2 + y^2 + 1$ је полином који зависи од две променљиве. Степени ових полинома имају нотацију $d°p$ $(degp)$, односно, $d°q$ $(degq)$. За полином ћемо рећи да је сређен по променљивој ако су његови чланови, тј. мономи, поређани по степенима у растућем или опадајућем поретку.

Над полиномима је могуће извршити рачунске операције сабирања и множења по следећим правилима.

Дефиниција 2.5. Структура $(\mathcal{Z}, +, \cdot)$ је интегрални домен ако је $\mathcal{Z}$ комутативан прстен са јединицом и за све $a, b \in \mathcal{Z}$ за које важи $a \cdot b = 0$ мора бити да је $a = 0$ или $b = 0$.

Дакле, у интегралном домену постоје делитељи нуле.

Дефиниција 2.6. Нека су дати полиноми:

$$a(x) = a_n x^x + \cdots + a_1 x + a_0 \text{ и } b(x) = b_m x^m + \cdots + b_1 x + b_0,$$

где је без умањења општости $d°a > d°b$, тада су збир и производ ових полинома задати са

$$a(x) + b(x) = a_n x^n + \cdots + a_{m+1} x^{m+1} + (a_m + b_m) x^m + \cdots + (a_1 + b_1) x + a_{0+} b_0$$

$$a(x) \cdot b(x) = \sum_{i=n}^{0}(a_i x^i \sum_{j=m}^{0} b_j x^j).$$

$$a(x) \cdot b(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + a_n b_m x^{m+n}$$

Степен збира два полинома биће мањи или једнак од максимума степена та два полинома, а степен производа два полинома биће једнак збиру њихових степена ако прстен $\mathcal{Z}$ нема праве делитеље нуле. Примећујемо да су збир и производ два полинома увек полином. Неутрални елемент за сабирање је нула полином, а супротни полином $a(x)$ је $-a(x)$, па се одузимање полинома не дефинише, већ се посматра као сабирање. Као количник два полинома не мора се увек јавити полином, те уводимо дељење са остатком, али најпре ћемо се подсетити дефиниције поља.

2.2. Делитељи полинома

Дефиниција 2.7. Уређена тројка $(\mathcal{Z}, +, \cdot)$ је поље ако важи:

1) $(\mathcal{Z}, +)$ је комутативна група;
2) $(\mathcal{Z} \setminus \{0\}, \cdot)$ је комутативна група;
3) за све $a, b, c \in \mathcal{Z}$ важи $a \cdot (b + c) = a \cdot b + a \cdot c$ и $(b + c) \cdot a = b \cdot a + c \cdot a$.

Пример 2.3. Структуре које ћемо навести јесу неке од могућих примера поља:

1. $(\mathbb{R}, +, \cdot)$ поље реалних бројева;
2. $(\mathbb{C}, +, \cdot)$ поље комплексних бројева;
3. $(\mathbb{Z}_p, +, \cdot)$ коначно поље целих бројева по модулу p, где је p прост број.

Из дефиниција 2.1. и 2.7. можемо закључити да су сва поља прстенови, али нису сви прстенови поља.

Како је $\mathcal{Z}$ поље, тако ће одговарајући прстен полинома бити комутативан и без правих делитеља нуле. Једини инверзибилни полиноми су не-нула константе.

Теорема 2.1. (Дељење са остатком) Ако је $\mathcal{Z}$ поље за полиноме $a(x)$ и $b(x)$ из $\mathcal{Z}[x]$, при чему је $b(x) \neq 0$, постоје јединствени полиноми $q(x)$ и $r(x)$ такви да је

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

при чему је степен полинома $r(x)$ строго мањи од степена полинома $b(x)$.

Уколико је водећи коефицијент полинома $b(x)$ инверзибилан, теорема важи и када је $\mathcal{Z}$ било који прстен.

Дефиниција 2.8. Одређивање полинома $q(x)$ и $r(x)$ називамо *левим еуклидским дељењем* полинома $a(x)$ полиномом $b(x)$, а саме полиноме $q(x)$ и $r(x)$ редом *количником* и *остатком* при дељењу.

Пример 2.4. При дељењу полинома $a(x) = x^3 + x + 1$ полиномом $b(x) = x^2 - x - 1$ количник је $q(x) = x + 1$, а остатак $r(x) = 3x + 2$.

Дефиниција 2.9. Полином $a(x)$ је дељив полиномом $b(x)$ у прстену $\mathbb{Z}[x]$ ако је остатак $r(x)$ при дељењу $a(x)$ са $b(x)$ једнак нула полиному. То значи да постоји полином $q(x)$ такав да је $a(x) = b(x)q(x)$. Тада кажемо још и да полином $b(x)$ дели полином $a(x)$.

Дефиниција 2.10. Нека су $a(x)$ и $b(x)$ полиноми прстена $\mathcal{Z}(x)$, где је $\mathcal{Z}$ поље. Полином $d(x)$ називамо заједничким делиоцем полинома $a(x)$ и $b(x)$ ако су и $a(x)$ и $b(x)$ дељиви са $d(x)$.

Дефиниција 2.11. Полином $d(x)$ је *највећи заједнички делилац* (**НЗД**) полинома $a(x)$ и $b(x)$ (који нису једнаки нули), ако је заједнички делилац тих полинома, уз то да је и сам дељив било којим другим делиоцем тих полинома.

Ако полином $d(x)$ задовољава наведене услове, онда и полином $k \cdot d(x)$ задовољава дате услове, где је k ненула елемент скупа $\mathcal{Z}$.

У већини случајева потребно је одредити такав полином $d(x)$, што нам осигурава *Еуклидов алгоритам*, односно, њиме потврђујемо јединственост таквог полинома.

Уколико полином $a(x)$ поделимо полиномом $b(x)$, добићемо следећу релацију:

$$a(x) = b(x)q_1(x) + r_1(x).$$

Затим настављамо дељење полинома $b(x)$ полиномом $r_1(x)$, који у овом случају представља остатак количника полинома $a(x)$ и $b(x)$, како бисмо добили следећу релацију:

$$b(x) = r_1(x)q_2(x) + r_2(x).$$

Поступак се тако наставља коначно много пута и добијамо низ остатака од којих је $r_k(x)$ последњи остатак различит од нуле и као такав представља највећи заједнички делилац.

Пример 2.5. Одреди НЗД $(x^5 + x^4 - x^3 - 3x^2 - 3x - 2 - 1, x^4 - 2x^3 - x^2 - 2x + 1)$.

Решење: Користимо Еуклидов алгоритам:

$(x^5 + x^4 - x^3 - 3x^2 - 3x - 2 - 1) : (x^4 - 2x^3 - x^2 - 2x + 1) = x + 3$

$[6x^3 + 2x^2 + 2x - 4]$

$(x^4 - 2x^3 - x^2 - 2x + 1) : (6x^3 + 2x^2 + 2x - 4) = \frac{1}{6}x - \frac{7}{18}$

$\left[-\frac{5}{9}x^2 - \frac{5}{9}x - \frac{5}{9}\right]$

$(6x^3 + 2x^2 + 2x - 4) : \left(-\frac{5}{9}x^2 - \frac{5}{9}x - \frac{5}{9}\right) = -\frac{54}{5}x + \frac{36}{5}$ [0].

Закључујемо да је

НЗД $(x^5 + x^4 - x^3 - 3x^2 - 3x - 2 - 1, x^4 - 2x^3 - x^2 - 2x + 1) = -\frac{5}{9}x^2 - \frac{5}{9}x - \frac{5}{9}$,

Односно, како је $-\frac{5}{9}x^2 - \frac{5}{9}x - \frac{5}{9} = -\frac{5}{9}(x^2 + x + 1)$, важи:

НЗД$(x^5 + x^4 - x^3 - 3x^2 - 3x - 2 - 1, x^4 - 2x^3 - x^2 - 2x + 1) = x^2 + x + 1$

Дефиниција 2.12. За полиноме $a(x)$ и $b(x)$ из прстена $\mathbb{Z}[x]$ кажемо да су узајмно прости ако је њихов највећи заједнички делилац једнак јединици.

Теорема 2.2. Нека је полином $d(x)$ највећи заједнички делилац полинома $p_1(x)$ и $p_2(x)$, који су елементи неког прстена $Z[x]$, где је Z поље, онда постоје полиноми $q_1(x)$ и $q_2(x)$ такви да је $d(x) = p_1(x)q_1(x) + p_2(x)q_2(x)$.

Пример 2.6. Дати су полиноми $p_1(x) = 3x^3 - 2x^2 + x + 2$ и $p_2(x) = x^2 - x + 1$. Одредити полиноме $q_1(x)$ и $q_2(x)$ тако да је:

$$p_1(x)q_1(x) + p_2(x)q_2(x) = 1.$$

Решење: Прво ћемо применити Еуклидов алгоритам на полиноме $p_1(x)$ и $p_2(x)$ и добити

$$p_1(x) = 3x^3 - 2x^2 + x + 2 = (3x + 1)(x^2 - x + 1) + (-x + 1),$$

$$p_2(x) = x^2 - x + 1 = (-x + 1)(-x) + 1.$$

Затим ћемо на десну страну једнакости додавати неопходне мономе како бисмо формирали тражене полиноме:

$$1 = x^2 - x^2 + x - x + 1 = x^2 - x + 1 - x(x - 1) = x^2 - x + 1 + x(-x + 1).$$

Сада ћемо из полинома $p_1(x)$ приметити да је:

$$-x + 1 = p_1(x) - (3x + 1)(x^2 - x + 1)$$

$$= x^2 - x + 1 + x[(3x^3 - 2x^2 + x + 2) - (3x + 1)(x^2 - x + 1)]$$

$$= x(3x^3 - 2x^2 + x + 2) + (x^2 - x + 1)\big(1 - x(3x + 1)\big)$$

$$= (3x^3 - 2x^2 + x + 2)x + (x^2 - x + 1)(-3x^2 - x + 1).$$

Стога имамо да је $q_1(x) = x$, а $q_2(x) = -3x^2 - x + 1$.

2.3. Нуле полинома

Дефиниција 2.13. Нека је a елемент поља $\mathcal{Z}$ такав да за фиксиран полином $p(x)$ из $\mathcal{Z}[x]$ важи $p(a) = 0$, тада се такво a назива нула или корен полинома.

Налажење нуле полинома подразумева одређивање решења једначине $p(a) = 0$, што у општем случају, када је полином степена пет или већег, није могуће. Специјалан случај за решавање једначине $ax^2 + bx + c = 0$ био је познат још у старом веку. Корене полинома добијамо по познатој формули:

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

Оно што представња проблем у вези са нулама полинома $p(x)$ из $\mathcal{Z}[x]$ јесте њихова локализација. То подразумева одређивање најмањих подскупова поља $\mathcal{Z}$ који ће садржати по тачно једну од тих нула.

Теорема 2.3. (Безуова теорема) Остатак који се добије при дељењу полинома $p(x)$ са $x-a$ једнак је $p(a)$. Закључујемо да је полином $p(x)$ дељив полиномом $x-a$ ако и само ако је $p(a)=0$.

Доказ: Означимо са $q(x)=x-a$. У општем случају дељење полинома $p(x)$ са $q(x)$ можемо записати као $p(x)=q(x)\cdot k(x)+r(x)$, где је $k(x)$ полином који представља количник, а $r(x)$ остатак. Дакле, полином $p(x)=(x-a)\cdot k(x)+r(x)$. Коначно, при случају $x=a$ добија се $p(a)=(a-a)\cdot k(a)+r(a)$, односно, $p(a)=r(a)$. □

2.4. Факторизација полинома

Када је реч о факторизацији полинома неконстантни полиноми са комплексним коефицијентима имају нулу у скупу комплексних бројева. Односно, важи следећа теорема:

Теорема 2.4. (О јединственој факторизацији) Полином $p(x)=a_nx^n+\cdots+a_1x+a_0$, где је $a_i\in\mathbb{C}, i=\overline{0,n}$ степена $n>0$ има бар једну нулу у пољу комплексних бројева и постоји јединствено представљање до на редослед чинилаца у облику:

$$p(x)=a_n(x-x_1)(x-x_2)\cdots(x-x_n),$$

где су $a_n\neq 0, x_1,\dots,x_n$ комплексни бројеви. Закључујемо да полином $p(x)$ има највише n различитих нула у пољу комплекснинх бројева.

Ово тврђење је, заправо, аналогно теореми о јединственој факторизацији природног броја на просте чиниоце.

Теорема 2.5. Полином $p(x)$ чији су коефицијенти реални бројеви има јединствену факторизацију до на редослед чинилаца у облику:

$$p(x)=a_n(x-x_1)\cdots(x-x_к)(x^2-p_1x+q_1)\cdots(x^2-p_lx+q_l),$$

где су x_i и p_j, q_j реални бројеви такви да $p_i^2<4q_i$ и $k+2l=n$.

Пример 2.7. Одреди факторизацију полинома $p(x) = x^4 + x^3 + x^2 + 3x - 6$ над пољем целих бројева.

Решење: Како је $p(1) = 0$, прво делимо полином $p(x)$ полиномом $x - 1$. Тада је:

$$(x^4 + x^3 + x^2 + 3x - 6) : (x - 1) = x^3 + 2x^2 + 3x + 6$$

Означимо са $q(x) = x^3 + 2x^2 + 3x + 6$. Како је $q(-2) = 0$, сада ћемо овај полином поделити са $x + 2$, добија се:

$$(x^3 + 2x^2 + 3x + 6) : (x + 2) = x^2 + x - 2.$$

Како последњи добијени полином нема целих нула, закључујемо да је факторизација полинома дата са:

$$p(x) = (x - 1)(x + 2)(x^2 + x - 2).$$

2.5. Својства полинома са целобројним коефицијентима

Нека је $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ полином такав да су му коефицијенти елементи скупа целих бројева, тада се разлика $p(x) - p(y)$ може написати у облику:

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

где можемо приметити да су сви сабирци дељиви полиномом $x - y$. Следећа теорема представља једно од важних аритметичких својстава полинома из $\mathbb{Z}[x]$:

Теорема 2.6. Нека је $p(x)$ полином са целобројним коефицијентима, тада је $p(a) - p(b)$ дељиво са $a - b$ за све различите целе бројеве a и b.

Из теореме можемо закључити да све целобројне нуле полинома $p(x)$ деле $p(0)$.

Пример 2.8. Доказати да полином $p(x)$ са целим коефицијентима нема целобројних нула ако узима вредности ± 1 у три различите целобројне тачке.

Решење: Претпоставимо супротно да су a, b, c и d цели бројеви такви да је $p(a), p(b), p(c) \in \{-1,1\}$ и $p(d) = 0$. Из теореме 2.6. закључујемо да $a-d, b-d$ и $c-d$ деле 1, што је контрадикција. □

За рационалне нуле полинома $p(x) \in \mathbb{Z}[x]$ важи следећа теорема:

Теорема 2.7. Ако је рационалан број $\frac{p}{q}$ $(p, q \in \mathbb{Z}, q \neq 0, \text{НЗД}\ (p, q) = 1)$ нула полинома

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ са целобројним коефицијентима, онда $p|a_0$ и $q|a_n$.

Доказ: Нека је $q^n f\left(\frac{p}{q}\right) = a_n p^n + \cdots + a_0 q^n$, тада видимо да су сви сабирци, осим, можда, првог дељиви са q и сви сабирици сем, можда, последњег дељиви са p. Према томе, тада је $a_n p^n$ дељив са q, а $a_0 q^n$ дељив са p, а како q не дели p^n, мора бити да $q|a_n$, слично тако $p|a_0$. □

Пример 2.9. Полином $p(x) = \frac{1}{2}x^2 - \frac{1}{2}x$ представља пример полинома који у свим целобројним тачкама узима целе вредности, али он није полином са целобројним коефицијентима.

3. Нерастављивост полинома

3.1. Нерастављивост полинома над прстеном целих бројева

Дефиниција 3.1. Полином $p(x) \in \mathbb{Z}[x]$ је *растављив* над $\mathbb{Z}[x]$ уколико постоје полиноми $a(x)$ и $b(x)$ из $\mathbb{Z}[x]$ позитивног степена такви да је $p(x) = a(x)b(x)$, уколико то није случај, кажемо да је полином $p(x)$ *нерастављив*, односно, *иредуцибилан*.

Исто тако се дефинише и нерастављивост над скупом рационалних или реалних бројева.

Следећа теорема коју ћемо навести представља уопштење теореме о јединственој факторизацији.

Теорема 3.1. Нека је $\mathcal{Z}$ поље. Сваки неконстантан полином $p(x) \in \mathcal{Z}(x)$ има факторизацију на нерастављиве полиноме и такво растављање је јединствено до на редослед чинилаца.

Пример 3.1. Сви полиноми са другим или трећим степеном који немају рационалинх нула биће нерастављиви над $\mathbb{Z}$. Такви су, на пример, полиноми $x^2 + x + 1$ и $x^3 + 2x^2 - 3x - 3$.

Дефиниција 3.2. Највећи заједнички делилац коефицијената $a_0, \dots, a_n$ полинома $p(x) \in \mathbb{Z}(x)$ зовемо садржитељем тог полинома у ознаци $cont(p)$. Јасно је да је $p(x) = cont(p)q(x)$, где је $q(x)$ полином над $\mathbb{Z}$ са садржитељем 1.

Теорема 3.2. $cont(ab) = cont(a)cont(b)$

Доказ: У случају да су садржатељи полинома a и b једнаки јединици, тврђење је тривијално. Нека је $A = \sum \alpha_i x^i$, $B = \sum \beta_i x^i$ и $AB = \sum \gamma_i x^i$. Претпоставимо да је $cont(AB) = d > 1$ и p прост број, тако да $p|d$. Тада су сви коефицијенти полинома AB дељиви са p. Претпоставимо да полиноми A и B немају све коефицијенте дељиве са p. Нека је α_r први коефицијент полинома A који није дељив са p, и β_s први коефицијент полинома B који није дељив са p.

Тада:

$$c_{r+s} = \alpha_r\beta_s + \alpha_{r+1}\beta_{s-1} + \alpha_{r+2}\beta_{s-2} + \cdots + \alpha_{r-1}\beta_{s+1} + \alpha_{r-2}\beta_{s+2} + \cdots$$

$$\equiv \alpha_r\beta_s \not\equiv 0 \pmod{p},$$

јер је:

$$\alpha_{r-1} \equiv \alpha_{r-2} \equiv \cdots \equiv \alpha_0 \equiv 0 \pmod{p},$$

$$\beta_{s-1} \equiv \beta_{s-2} \equiv \cdots \equiv \beta_0 \equiv 0 \pmod{p}.$$

Дошли смо до контрадикције, па можемо претпоставити да су сви коефицијенти полинома A дељиви са p. Ако полином A поделимо са p и наставимо на сличан начин, долазимо до жељеног резултата. □

3.2. Гаусова лема

Теорема 3.3. (Гаусова лема) Полином чији су коефицијенти цели бројеви је иредуцибилан над $\mathbb{Z}$ ако и само ако је иредуцибилан над $\mathbb{Q}$.

Доказ: Нека је $a(x) \in \mathbb{Z}[x]$ и $a(x) = b(x)c(x)$, где $b(x), c(x) \in \mathbb{Q}[x]$. Поред тога, претпоставићемо и да је $cont(a) = 1$. Изабраћемо m позитиван цео број такав да је $mb(x) \in \mathbb{Z}[x]$. Нека је $n = cont(mb)$. Тада је број $r = \frac{m}{n}$ такав да је $rb(x) \in \mathbb{Z}[x]$ и $cont(rb) = 1$. Слично ћемо изабрати и позитиван рационалан број s за полином $c(x)$. Докажимо сада да је $rs = 1$. Како је $(rb(x))(sc(x))$ факторизација полинома $rsa(x)$ над $\mathbb{Z}$, на основу теореме 3.2. $cont(rb)cont(sc) = cont(rsbc)$, односно, $1 = cont(rsa)$. Како је $cont(a) = 1$, закључујемо да је $rs = 1$. Дакле, $a(x) = \big(rb(x)\big)(sc(x))$ је факторизација полинома $a(x)$ у $\mathbb{Z}[x]$, чиме је доказ завршен. □

4. Критерјуми нерастављивости полинома над прстеном целих бројева

4.1. Ајзенштајнов критеријум

Теорема 4.1. (Ајзенштајнов критеријум) Нека је $p(x) = a_0 + a_1x + \cdots + a_nx^n$ полином такав да је $a_i \in \mathbb{Z}$. Уколико за такав полином важи да су му коефицијенти $a_0, \dots, a_{n-1}$ дељиви простим бројем p, а a_n није дељив са p и a_0 није дељив са p^2, тада је $p(x)$ нерастављив над $\mathbb{Z}$.

Доказ: Претпоставимо да:

$$p(x) = g(x)h(x) = (\sum b_k x^k)(\sum c_l x^l),$$

тако да су $g(x)$ и $h(x)$ полиноми чији је степен природан број са целобројним коефицијентима. Број $b_0c_0 = a_0$ је дељив бројем p, из чега следи да је b_0 или c_0 дељив бројем p. Без умањења општости узмимо да је b_0 дељив бројем p. Тада c_0 није дељив са p, јер a_0 није дељив са p^2. Ако би сви коефицијенти b_i били дељиви са p, онда би и a_n био дељив са p. Зато нека b_i није дељив са p за неко i, $1 \leq i \leq degg < n$. Претпоставимо да је i последњи индекс бројева b_i који нису дељиви са p. Са једне стране, према претпоставци, a_i је дељив бројем p. Са друге стране, $a_i = b_ic_0 + b_{i-1}c_1 + \cdots + b_0c_i$, где су сви сабирци, осим b_ic_0, дељиви са p, чиме се долази до контрадикције. □

Пример 4.1. Доказати да је полином $p(x) = x^3 - 14x + 7$ нерастављив над $\mathbb{Z}$.

Решење: Како $7|7$ и $7|-14$, а $7 \nmid 1$ и $7^2 \nmid 7$ полином $p(x)$ је нерастављив над $\mathbb{Z}$.

Пример 4.2. Користећи Ајзенштајнов критеријум доказати да је следећи полином

$$p(x) = x^4 - x^3 + 2x + 1$$

нерастављив.

Решење: Прво ћемо разложити полином користећи Тејлоров развој. Добићемо да је:

$$p(x) = (x-1)^4 + 3(x-1)^3 + 3(x-1)^2 + 3(x-1) + 3.$$

Затим уводимо смену $x = t + 1$ и добијамо да је:

$$q(t) = p(t + 1) = t^4 + 3t^3 + 3t^2 + 3t + 3.$$

На основу Ајзенштајновог критеријума, где је $p = 3$, полином $q(t)$ је нерастављив, па је и полином $p(x)$ такав. Када он не би био нерастављив, постојали би полиноми $u(x)$и $v(x)$ такви да је $p(x) = u(x) \cdot v(x)$, $d°u, d°v > 0$. Сменом $x = t + 1$ у последњој једнакости добијамо да је $p(t + 1) = u(t + 1) \cdot v(t + 1) = u_1(t) \cdot v_1(t)$, где су $u_1(t)$ и $v_1(t)$ полиноми степена већег од нуле. Ово је у контрадикцији са чињеницом да је полином $q(t) = p(t + 1)$ нерастављив.

На први поглед није јасно како применити Ајзенштајнов критеријум. Како се сваки полином може развити по степенима $x - x_0, x_0 \in \mathbb{R}$, нормално је потражити x_0 тако да се Ајзенштајнов критеријум може применити на полином развијен по степенима $x - x_0$, јер се сменом $x = t + x_0$ полином изражава преко степена t. Одређивање броја x_0 је уствари проблем који се тешко решава. Најједноставније је написати све изводе датог полинома, па одатле покушати да се одреди број x_0, за који ће коефицијенти у полиному задовољавати Ајзенштајнов критеријум.

Пример 4.3. Ако је p прост број, доказати да је полином $p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ нерастављив.

Решење: Множењем датог полинома полиномом $x - 1$ добијамо једнакост:

$$(x - 1)p(x) = x^p - 1.$$

Након увођења смене $x = t + 1$ полином $p(t + 1)$ ћемо означити са $q(t)$. Сада је:

$$tq(t) = tp(t + 1) = (t + 1)^p - 1 = t^p + \binom{p}{1} t^{p-1} + \binom{p}{2} t^{p-2} + \cdots + \binom{p}{p-1} t.$$

Када ову једнакост поделимо са t уочавамо да су сви биномни коефицијенти дељиви са p и да $p \nmid 1$ и $p^2 \nmid p$, па је самим тим полином $q(t)$ нерастављив на основу Ајзенштајновог критеријума, а тиме је нерастављив и полином $p(x)$, чија се нерастављивост доказује аналогно претходном примеру.

Пример 4.4. Доказати да је дати полином $f(x)$ нерастављив, где је p прост број.

$$f(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1}$$

Решење: Да бисмо применили Ајзенштајнов критеријум за прост број p, уводимо смену $x = t + 1$ и доказујемо да је полином:

$$f(t+1) = q(t) = \frac{(t+1)^{p^k} - 1}{(t+1)^{p^{k-1}} - 1}$$

нерастављив. Како је:

$$q(t) = (t+1)^{(p-1)p^{k-1}} + (t+1)^{(p-2)p^{k-1}} + \cdots + (t+1)^{p^{k-1}} + 1$$

закључујемо да је водећи коефицијент полинома $q(t)$ једнак 1, док је слободан члан једнак p и дељив је са p, а није дељив са p^2. Докажимо да су сви остали коефицијенти дељиви са p. Показаћемо да су сви коефицијенти полинома $(t+1)^{p^k} - 1$, осим водећег, дељиви са p. Доказ ћемо завршити индукцијом. За $k = 1$ тврђење важи на основу примера 4.3. Претпоставимо да је тврђење тачно за $k = n - 1$. У том случају можемо писати да је:

$$(t+1)^{p^{n-1}} - 1 = t^{p^{n-1}} + ph_{n-1}(t),$$

где је $h_{n-1}(t)$ неки полином са целобројним коефицијентима. Користећи индуктивну хипотезу добијамо да је:

$$(t+1)^{p^n} = \left(t^{p^{n-1}} + 1 + ph_{n-1}(t)\right)^p = \left(t^{p^{n-1}} + 1\right)^p + p\varphi(t) = t^{p^n} + 1 + ph_n(t),$$

где су $h_n(t)$ и $\varphi(t)$ полиноми са целобројним коефицијентима. Сада имамо да је:

$$q(t) = \frac{t^{p^k} + ph_k(t)}{t^{p^{k-1}} + ph_{k-1}(t)} = t^{(p-1)p^{k-1}} + \frac{p\left(h_k(t) - t^{(p-1)p^{k-1}} h_{k-1}(t)\right)}{t^{p^{k-1}} + ph_{k-1}(t)} = t^{(p-1)p^{k-1}} + p\psi(t),$$

где су коефицијенти полинома $\psi(t)$ целобројни, јер је $\psi(t)$ количник полинома са целобројним коефицијентима, при чему је водећи коефицијент делиоца једнак 1. Међутим, примећујемо да су сви коефицијенти полинома $q(t)$, осим водећег, дељиви са p. Сви услови

Ајзенштајновог критеријума за полином $q(t)$ су задовољени, па је он нерастављив, те је такав и полином $f(t+1)$. Одатле следи нерастављивост полинома $f(x)$.

Пример 4.5. Доказати да је полином $f(x) = x^n + 5x^{n-1} + 3, n > 1$ нерастављив у скупу полинома са целобројним коефицијентима.

Решење: Претпоставимо супротно, да постоје ненула полиноми $g(x)$ и $h(x)$ са целобројним коефицијентима такви да је $f(x) = g(x)h(x)$. Како је $|f(0)| = 3$, следи да је $|g(0)| = 1$ или $|h(0)| = 1$. Без умањења општости узмимо да је $|g(0)| = 1$ и нека је $g(x) = (x - x_1)(x - x_2) \cdot \ldots \cdot (x - x_k)$, где је $x_i \in \mathbb{C}$. Тада је $|x_1 x_2 \cdot \ldots \cdot x_k| = 1$. Како је $x_i^{n-1}(x_i + 5) = -3$ за свако $i = 1,2, \ldots, k$ множењем ових једнакости добијамо да је $|(x_1 + 5)(x_2 + 5) \cdot \ldots \cdot (x_k + 5)| = |g(-5)| = 3^k$. Међутим, $f(-5) = g(-5)h(-5) = 3$, па је $d°g(x) = k = 1$. У том случају полином $f(x)$ има целобројну нулу. Полином $f(x)$ нема целобројне нуле, што је лако проверити, па добијена контрадикција доказује тврђење задатка.

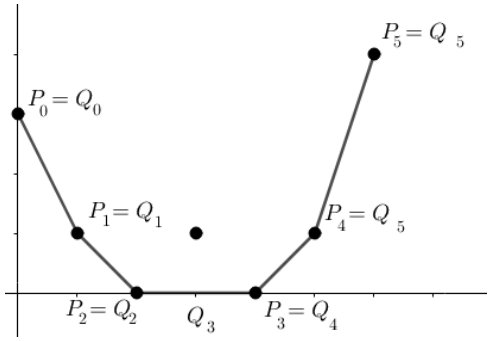
4.2. Думин критеријум иредуцибилности

Нека је p фиксиран прост број и $f(x) = \sum_{i=0}^{n} A_i x^i$ полином са целобројним коефицијентима такав да $A_0 A_n \neq 0$. Означимо ненула коефицијенте полинома $f(x)$ са $A_i = a_i p^{\alpha_i}$, тако да су a_i цели бројеви који нису дељиви са p. Сваком ненула коефицијенту $a_i p^{\alpha_i}$ доделићемо тачке, тј. уређени пар координата (i, α_i). Ове тачке ће нас довести до *Њутновог дијаграма полинома* $f(x)$ (који зависи од p).

Нека је $P_0 = (0, \alpha_0)$ и $P_1 = (i_1, \alpha_{i_1})$, где је i_1 највећи цео број за који важи да нема тачака (i, α_i) испод линије $P_0 P_1$. Даље, нека је $P_2 = (i_2, \alpha_{i_2})$, где је i_2 највећи цео број за који важи да нема тачака (i, α_i) испод линије $P_1 P_2$, итд. Последња дуж је облика $P_{r-1} P_r$, тако да $P_r = (n, \alpha_n)$. Уколико нека дуж изломљене линије $P_0 \ldots P_r$ пролази кроз тачку са целобројном координатом, тада ће та тачка бити сматрана за теме ове изломљене линије. Оваквим исцртавањем теменима $P_0, \ldots, P_r$ се додаје $s \geq 0$ темена. Резултат је изломљена линија $Q_0 \ldots Q_{r+s}$ коју називамо Њутновим дијаграмом. Дужи $P_l P_{l+1}$ и $Q_i Q_{i+1}$ ћемо називати

страницама, односно, дужима Њутновог дијаграма, тим редом, а векторе $\overrightarrow{Q_lQ_{l+1}}$ векторима дужи Њутновог дијаграма. Можемо приметити да коефицијенти правца правих који садрже ове векторе формирају неопадајући низ.

Дефиниција 4.1. Систем вектора дужи Њутновог дијаграма полинома $f(x)$ је фамилија његових дужи, при чему се сваки вектор узима са вишеструкошћу с којом се појављује у Њутновом дијаграму.



Теорема 4.2. Нека је $f(x) = g(x)h(x)$, тако да су $f(x), g(x)$ и $h(x)$ полиноми са целобројним коефицијентима. Тада је систем вектора за полином $f(x)$ једнак унији система вектора за полиноме $g(x)$ и $h(x)$ (уз услов да је p исто за све полиноме).

Доказ: Нека су:

$$f(x) = \sum_{i=0}^{n} a_i p^{\alpha_i} x^i, \quad g(x) = \sum_{j=0}^{m} b_j p^{\beta_j} x^j, \quad h(x) = \sum_{k=0}^{n-m} c_k p^{\gamma_k} x^k,$$

такви да су a_i, b_j, c_k бројеви који нису дељиви са p. Посматраћемо Њутнов дијаграм полинома $f(x)$. Нека су координате неких тачака P_l и P_{l+1} редом (i_-, α_{i_-}) и (i_+, α_{i_+}). Нагиб дужи P_lP_{l+1} можемо израчунати на следећи начин:

$$M = \frac{\alpha_{i_+} - \alpha_{i_-}}{i_+ - i_-}.$$

Нека је $\alpha_{i_+} - \alpha_{i_-} = At$ и $i_+ - i_- = It$, тако да је $t > 0$, највећи заједнички делилац бројева $\alpha_{i_+} - \alpha_{i_-}$ и $i_+ - i_-$. Тада је $M = \frac{A}{I}$, при чему је $(A, I) = 1$.

Страна P_lP_{l+1} Њутновог дијаграма је део праве

$$I\alpha - Ai = F, \text{ где је } F = I\alpha_{i_+} - Ai_+ = I\alpha_{i_-} - Ai_-.$$

Према претпоставци све тачке (i, α_i), тако да је $i = \overline{0,n}$, леже на или изнад ове линије, тј. $I\alpha_i - Ai \geq F$, где је строга неједнакост за $i < i_-$ и $i > i_+$.

Број $I\alpha_i - Ai$ ћемо назвати тежином монома $ap^\alpha x^i$, где је $(a,p) = 1$. Бројеви i_+ и i_- су јединствено условљени као најмањи и највећи експонент степена x за све мономе који се јављају у полиному $f(x)$ са најмањом тежином.

За полином $g(x)$ размотрићемо:

$$G = \min_{j=0,\dots,m}\{I\beta_j - \mathrm{Aj}\}$$

и дефинисаћемо j_- и j_+ као најмањи и највећи индекс за који

$$G = I\beta_{j_-} - Aj_- = I\beta_{j_+} - Aj_+.$$

Слично, за полином $h(x)$ ћемо размотрити:

$$H = \min_{k=0,\dots,n-m}\{I\gamma_k - Ak\},$$

и дефинисаћемо k_- и k_+ као најмањи и највећи индекс за који је

$$H = I\gamma_{k_-} - Ak_- = I\gamma_{k_+} - Ak_+.$$

Јасно је да

$$a_{j_-+k_-}p^{\alpha_{j_-+k_-}} = \sum_{j+k=j_-+k_-}\left(b_j p^{\beta_j}x^j\right)\left(c_k p^{\gamma_k}x^k\right).$$

Тежина производа два члана једнака је збиру њихових тежина и зато је тежина сабирака са $j = j_-$ и $k = k_-$ једнака $G + H$. Тежина свих осталих сабирака је строго већа од $G + H$, због тога што је $j < j_-$ или $k < k_-$.

Заиста, нека је, на пример, $j < j_-$. Тада је тежина $b_j p^{\beta_j}x^j$ строго већа од G и тежина $c_k p^{\gamma_k}x^k$ није мања од H.

Тежина производа $\left(b_j p^{\beta_j} x^j\right)\left(c_k p^{\gamma_k} x^k\right)$ за $j+k=const$ монотоно расте како $\beta_j+\gamma_k$ расте, јер је $I>0$. У случају када је $j+k=j_-+k_-$ сума $\beta_j+\gamma_k$ је минимална једино за $j=j_-$ и $k=k_-$. Зато је тежина коефицијента $a_{j_-+k_-}p^{\alpha_{j_-+k_-}}$ једнака $G+H$.

Такође, јасно је да је за $i<j_-+k_-$ тежина $a_i p^{\alpha_i}x^i$ строго већа од $G+H$, где заправо за $i\geq j_-+k_-$ тежина $a_i p^{\alpha_i}x^i$ није мања од $G+H$. Стога, $G+H=F$ и $j_-+k_-=i_-$. Слично доказујемо и да је $j_++k_+=i_+$. Односно,

$$i_+-i_-=(j_+-j_-)+(k_+-k_-).$$

Посебно, један од сабирака j_+-j_- и k_+-k_- је различит од нуле. Уколико су оба сабирка различита од нуле, тада је дуж чије су крајње тачке (j_-,β_{j_-}) и (j_+,β_{j_+}) страница Њутновог дијаграма за полином $g(x)$ и дуж са крајњим тачкама (k_-,γ_{k_-}) и (k_+,γ_{k_+}) је страница Њутновог дијаграма за полином $h(x)$. Нагиб обе дужи је једнак $M=\frac{A}{I}$, јер је

$$\frac{\beta_{j_+}-\beta_{j_-}}{j_+-j_-}=\frac{A}{I}=\frac{\gamma_{k_+}-\gamma_{k_-}}{k_+-k_-}.$$

Из $i_+-i_-=(j_+-j_-)+(k_+-k_-)$ видимо да је збир дужина страница чији је нагиб M Њутновог дијаграма полинома $g(x)$ и $h(x)$ једнак дужини странице истог нагиба M Њутновог дијаграма полинома $f(x)$.

Уколико један од сабирака j_+-j_- или k_+-k_- изоставимо, тада ће Њутнов дијаграм за један од полинома, $g(x)$ или $h(x)$, имати страницу са нагибом M и његова дужина ће бити једнака дужини странице Њутновог дијаграма полинома $f(x)$, где Њутнов дијаграм другог полинома нема страницу са нагибом M.

Закључујемо да је вектор странице са нагибом M Њутновог дијаграма за полином $f(x)$ једнак збиру вектора страница са истим нагибом M Њутновог дијаграма за полиноме $g(x)$ и $h(x)$. Из једнакости $i_+-i_-=(j_+-j_-)+(k_+-k_-)$ видимо да, уколико један од Њутнових дијаграма за полиноме $g(x)$ и $h(x)$ садржи страницу са одређеним нагибом M, тада ће Њутнов дијаграм за полином $f(x)$ такође поседовати страницу са истим нагибом. □

Последица: Ако се за прост број p Њутнов дијаграм полинома $f(x)$ састоји од тачно једне дужи, односно, од дужи која не садржи тачке са целобројним координатама, тада је полином $f(x)$ нерастављив.

Пример 4.6. (Ајзенштајнов критеријум) Нека је $f(x) = a_0 + a_1x + \cdots + a_nx^n$ полином такав да је $a_i \in \mathbb{Z}$. Уколико за такав полином важи да су му коефицијенти $a_0, \dots, a_{n-1}$ дељиви простим бројем p, а a_n није дељив са p и a_0 није дељив са p^2, тада је $f(x)$ нерастављив над $\mathbb{Z}$.

Доказ: Њутнов дијаграм полинома $f(x)$ садржи тачно једну дуж чије су координате крајњих тачака $(0,1)$ и $(n,0)$. Ова дуж не садржи тачке са целобројним координатама. □

Пример 4.7. Нека је p прост број, $(c,p) = 1$ и $(m,n) = 1$, тада је полином $x^n + cp^m$ нерастављив.

Доказ: Њутнов дијаграм полинома $x^n + cp^m$ је дуж чије су координате крајњих тачака $(0,m)$ и $(n,0)$. Како су m и n узајамно прости бројеви, нема тачака на дијаграму са целобројним координатама, па је тај полином нерастављив. □

Пример 4.8. Нека је p прост број. Ако полином $f(x) = x^n + px + bp^2$, где су b и p узајамно прости бројеви, нема целобројних нула, онда је он нерастављив.

Доказ: Њутнов дијаграм полинома $f(x) = x^n + px + bp^2$ је унија дужи чије су крајње тачке $(0,2)$ и $(1,1)$ и дужи чије су крајње тачке $(1,1)$ и $(n,0)$. Како ове дужи не садрже тачке са целобројним координатама, факторизација полинома $f(x)$ над $\mathbb{Z}$ састоји се само од линеарног фактора и фактора степена $n-1$, што није могуће јер $f(x)$ нема целобројних нула. □

4.3. Полиноми са доминантним коефицијентима

У специјалним случајевима може се гарантовати да ће полином са одређеним „великим" коефицијентима бити нерастављив. Од свих критеријума овог типа, најпознатији је Перонов критеријум о ком ћемо говорити.

Теорема 4.3. Нека је $p(x) = x^n + a_1x^{n-1} + \cdots + a_n$ полином са целобројним коефицијентима такав да је $a_n \neq 0$.

а) Ако је $|a_1| > 1 + |a_2| + \cdots + |a_n|$, тада је $p(x)$ нерастављив.

б) Ако је $|a_1| \geq 1 + |a_2| + \cdots + |a_n|$, и $p(\pm 1) \neq 0$, тада је $p(x)$ нерастављив.

Доказ: а) Прво ћемо доказати да све нуле полинома $p(x)$, осим тачно једне, леже унутар диска $|z| \leq 1$. Јасно је да полином

$$q(x) = x^n + a_1x^{n-1}$$

задовољава ово својство, тј. да све нуле полинома $q(x)$, осим тачно једне, леже унутар диска $|z| \leq 1$. Зато је, по Рушеовом ставу, довољно доказати да за $|z| = 1$ имамо:

$$|p(z) - q(z)| < |p(z)| + |q(z)|.$$

Заиста за $|z| = 1$ имамо, са једне стране,

$$|p(z) - q(z)| = |a_2z^{n-2} + \cdots + a_n| \leq |a_2| + \cdots + |a_n| < |a_1| - 1,$$

а са друге стране

$$|p(z)| + |q(z)| \geq |q(z)| = |z^n + a_1z^{n-1}| = |z + a_1| \geq |a_1| - 1.$$

Докажимо сада да је $p(x)$ иредуцибилан. Претпоставимо супротно, да полином $p(x)$ можемо представити као производ полинома $p_1(x)$ и $p_2(x)$ чији је степен већи од нуле са целобројним коефицијентима. Производ нула сваког од ових полинома је ненула цео број и зато сваки од ових полинома има нулу чији модул није мањи од 1. Али полином $p(x)$ има само једну такву нулу, па зато долазимо до контрадикције.

б) Ако је $|a_1| = 1 + |a_2| + \cdots + |a_n|$, тада важи неједнакост:

$$|p(z) - q(z)| = |a_2z^{n-2} + \cdots + a_n| \leq |a_2| + \cdots + |a_n| \leq |a_1| - 1,$$

али ако $p(\pm 1) \neq 0$, тада ће важити да:

$$|p(z)| + |q(z)| > |q(z)| = |z^n + a_1z^{n-1}| = |z + a_1|.$$

Заиста, за $|z| = 1$ једнакост

$$|p(z)| + |q(z)| = |a_1| - 1$$

је једино могућа када је $|p(z)| = 0$ и $|z + a_1| = |a_1| - 1$. Последња једнакост једино је могућа за $z \in \mathbb{R}$. Како је $|z| = 1$, следи да је $z = \pm 1$, али тада $p(z) \neq 0$. □

Теорема 4.4. Нека су $a_1 \geq a_2 \geq \cdots \geq a_n$ природни бројеви и $n \geq 2$. Тада је полином $p(x) = x^n - a_1 x^{n-1} - a_2 x^{n-2} - \cdots - a_n$ нерастављив над $\mathbb{Z}$.

Доказ: Посматраћемо полином $f(x) = (x-1)p(x)$. Јасно је да:

$$f(x) = x^{n+1} - b_1 x^n + b_2 x^{n-1} + \cdots + b_{n+1},$$

где су $b_1 = a_1 + 1, b_2 = a_1 - a_2, \ldots, b_n = a_{n-1} - a_n, b_{n+1} = a_n$. Бројеви $b_1, \ldots, b_{n+1}$ су ненегативни цели бројеви и $b_1 = 1 + b_2 + \cdots + b_{n+1}$. Зато $f(x)$ задовољава први од услова дела (б) претходне теореме, али не задовољава други услов, јер је $f(1) = 0$, те ћемо користити други аргумент. Нека је:

$$h(z) = b_1 z^n - b_2 z^{n-1} - \cdots - b_{n+1}.$$

Прво ћемо показати да за довољно мало $\varepsilon > 0$, имамо следеће:

$$|h(z)| > |z^{n+1}| = |f(z) + h(z)|$$

свуда на кружници $|z| = 1 + \varepsilon$. Ако $|z| = 1 + \varepsilon$, тада:

$$|h(z)| - |z^{n+1}| \geq b_1(1+\varepsilon)^n - b_2(1+\varepsilon)^{n-1} - \cdots - b_{n+1} - (1+\varepsilon)^{n+1} =$$

$$\varepsilon\big(nb_1 - (n-1)b_2 - \cdots - 2b_{n-1} - b_n - (n+1)\big) + \cdots =$$

$$\varepsilon(b_2 + 2b_3 + \cdots + (n-1)b_n + nb_{n+1} - 1) + \cdots$$

Коефицијент ε је позитиван, али зато за довољно мало $\varepsilon > 0$ имамо $|h(z)| - |z^{n+1}| > 0$. У овом случају:

$$|f(z) + h(z)| = |z^{n+1}| < |h(z)| \leq |f(z)| + |h(z)|.$$

Зато полином $f(z)$ има онолико нула унутар диска $|z| \leq 1 + \varepsilon$ колико их има и $h(z)$. Али нуле полинома $h(z)$ леже искључиво унутар диска $|z| \leq 1$. Уколико $|z| \geq 1$, тада:

$$|h(z)| \geq b_1|z|^n - b_2|z|^{n-1} - \cdots - b_{n+1} \geq |z|^n(b_1 - b_2 - \cdots - b_{n+1}) = |z|^n > 0.$$

Ако пустимо да $\varepsilon \to 0$, видимо да унутар и на граници диска $|z| = 1$ имамо тачно n нула полинома $f(x) = (x-1)p(x)$. Како су тачно $n-1$ нула полинома $p(x)$ унутар диска, то значи да тачно једна нула мора лежати ван диска. Као у доказу претходне теореме закључујемо да полином $p(x)$ мора бити нерастављив. □

Теорема 4.5. Нека је $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x \pm p$ полином са целобројним коефицијентима, а p прост број.

а) Ако је $p > 1 + |a_1| + \cdots + |a_{n-1}|$, тада је полином $f(x)$ нерастављив.

б) Ако је $p \geq 1 + |a_1| + \cdots + |a_{n-1}|$ и полином $f(x)$ нема нула модула 1, тада је полином $f(x)$ нерастављив.

Доказ: Претпоставимо да је $f(x) = g(x)h(x)$, тако да су полиноми $g(x)$ и $h(x)$ степена већег од нуле са целобројним коефицијентима. Производ слободних чланова полинома $g(x)$ и $h(x)$ једнак је $\pm p$. Како је p прост број, један од слободних чланова ових полинома једнак је ± 1. Зато је производ модула нула једног од полинома $g(x)$ и $h(x)$ једнак 1. Један од полинома зато мора имати нулу α такву да је $|\alpha| \leq 1$. Како је α такође и нула полинома $f(x)$, из $f(\alpha) = 0$ следи да је:

$$p = |\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha| \leq 1 + |a_1| + \cdots + |a_{n-1}|.$$

У случају под а) дошли смо до контрадикције.

У случају под б) α није модула 1, већ је $|\alpha| < 1$, па је $p < 1 + |a_1| + \cdots + |a_{n-1}|$, односно, опет смо дошли до контрадикције. □

5. Примери полинома који не подлежу наведеним критеријумима

Пример 5.1. Ако полином трећег степена нема рационалних нула, доказати да је он нерастављив над прстеном $\mathbb{Z}$.

Решење: Ако би полином трећег степена био растављив у скупу $\mathbb{Z}[x]$, онда би један фактор у том разлагању био полином првог степена са целобројним коефицијентима, па би полином имао бар један рационалан корен, што је у контрадикцији са поставком задатка.

Пример 5.2. Доказати да се полином $f(x) = x^4 + 2x^2 + 2x + 2$ не може приказати као производ два полинома другог степена са целобројним коефицијентима.

Решење: Претпоставимо да се полином $f(x)$ може приказати као производ полинома $x^2 + ax + b$ и $x^2 + cx + d$ са целобројним коефицијентима. Тада имамо да је:

$(x^2 + ax + b) \cdot (x^2 + cx + d) = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (bc + ad)x + bd$
односно,

$$a + c = 0,$$

$$b + ac + d = 2,$$

$$bc + ad = 2,$$

$$bd = 2.$$

Како су a, b, c, d цели бројеви, из последње једнакости закључујемо да један од коефицијената b или d мора бити једнак ± 1, док други мора бити ± 2 и да су истог знака. Нека је нпр. $|b| = 1, |d| = 2$. Тада из треће једнакости следи да је bc парно. Како је b непарно, мора бити да је c парно. Онда због прве једнакости следи да је a парно. Овим смо добили да је сада $b + ac + d$ непарно, што је у контрадикцији са другом једначином. Како $f(x)$ нема целобројних нула овиме смо доказали да се дати полином не може представити као производ два полинома са целобројним коефицијентима.

Пример 5.3. Ако су $a_1, a_2, \dots, a_n$ међусобно различити цели бројеви, доказати да је полином

$$f(x) = (x - a_1)(x - a_2) \cdot \dots \cdot (x - a_n) - 1$$

нерастављив.

Решење: Нека је $f(x) = g(x)h(x)$, где су $g(x)$ и $h(x)$ полиноми са целобројним коефицијентима, чији су степени барем 1. Како је $f(a_i) = -1$, или је $g(a_i) = 1$, а $h(a_i) = -1$, или је $g(a_i) = -1$, а $h(a_i) = 1$. У оба случаја је $g(a_i) + h(a_i) = 0$ за свако $i = 1,2, \dots, n$. Како је $f(x) = g(x)h(x)$, степени полинома $g(x)$ и $h(x)$ мањи су од n, па је степен полинома $g(x) + h(x)$ такође мањи од n. Пошто је број нула полинома $g(x) + h(x)$ већи од степена овог полинома, на основу познатог става полином $g(x) + h(x)$ је идентички једнак нула полиному. Стога је $g(x) = -h(x)$, па је $f(x) = -h^2(x)$, што је у контрадикцији са чињеницом да је водећи коефицијент полинома $f(x)$ једнак 1.

Пример 5.4. Ако су $a_1, a_2, \dots, a_n$ међусобно различити цели бројеви, доказати да је полином

$$f(x) = (x - a_1)(x - a_2) \cdot \dots \cdot (x - a_n) + 1$$

нерастављив, осим полинома

$$(x - a)(x - a - 1)(x - a - 2)(x - a - 3) + 1 = ((x - a - 1)(x - a - 2) - 1)^2$$

и $(x - a)(x - a - 2) + 1 = (x - a - 1)^2$.

Решење: Претпоставимо да полином није нерастављив. Тада се он може приказати као производ полинома $g(x)$ и $h(x)$ чији су степени већи од нуле. Како је $f(a_i) = 1$, следи да је $g(a_i) = h(a_i) = \pm 1$. Како полиноми $g(x)$ и $h(x)$ нису константе, њихови степени су мањи од n, а ако им се вредности поклапају у n различитих тачака, следи да су они идентички једнаки. Стога је

$$f(x) = g^2(x).$$

Ова једнакост могућа је једино ако је n парно. Из исте следи једнакост:

$$(x - a_1)(x - a_2) \cdot \dots \cdot (x - a_n) = (g(x) + 1)(g(x) - 1),$$

из које добијамо да је, рецимо,

$$g(x) + 1 = (x - a_1)(x - a_3) \cdot \dots \cdot (x - a_{n-1})$$

$$g(x) - 1 = (x - a_2)(x - a_4) \cdot \dots \cdot (x - a_n).$$

Одузимањем ових једнакости имамо да је:

$$(x-a_1)(x-a_3)\cdot\ldots\cdot(x-a_{n-1})-(x-a_2)(x-a_4)\cdot\ldots\cdot(x-a_n)=2$$

Како су цели бројеви $a_1, a_2, \ldots, a_n$ различити, можемо претпоставити да је, рецимо, $a_1 > a_3 > \cdots > a_{n-1}$. Ако у последњој једнакости ставимо да је $x = a_{2k}$, где је $k = 1,2,\ldots,\frac{n}{2}$ добићемо следећу једнакост:

$$(a_{2k}-a_1)(a_{2k}-a_3)\cdot\ldots\cdot(a_{2k}-a_{n-1})=2.$$

У овој једнакости сви фактори разлагања броја 2 су различити, а поређани су у растућем низу. На тај начин смо добили $\frac{n}{2}$ различитих разлагања броја 2 са $\frac{n}{2}$ целих фактора поређаних у растућем поретку. Ово је могуће само за $\frac{n}{2}=2$, то јест $2=-2(-1)=1\cdot 2$, и за $\frac{n}{2}=1$. Управо то су наведени случајеви када је полином $f(x)$ растављив. У свим осталим случајевима он је нерастављив.

Пример 5.5. Ако полином $f(x)$ $n-$тог степена са целобројним коефицијентима има вредности ± 1 у више од $2m$ целобројних вредности променљиве, где је $n = 2m$ или $n = 2m+1$, доказати да је он нерастављив.

Решење: Претпоставимо да полином $f(x)$ није нерастављив. Тада се он може приказати као производ полинома $g(x)$ и $h(x)$ чији су степени барем 1. Степен једног од њих није већи од m, јер би у противном степен полинома $f(x)$ био већи од $2m+1$. Не умањујући општост разматрања, можемо претпоставити да степен полинома $g(x)$ није већи од m. Како полином $f(x)$ има вредности ± 1 за више од $2m$ целобројних вредности променљиве, те исте вредности мора имати и полином $g(x)$. Једну од вредности ± 1 полином $g(x)$ добија за више од m целобројних вредности променљиве. Но, онда је полином идентички једнак тој вредности на основу познатог става. Ово је у контрадикцији са претпоставком да полином $f(x)$ није нерастављив.

Пример 5.6. Ако су $a_1, a_2, \ldots, a_n$ међусобно различити цели бројеви, доказати да је полином

$$f(x)=(x-a_1)^2(x-a_2)^2\cdot\ldots\cdot(x-a_n)^2+1$$

нерастављив.

Решење: Приметимо, најпре, да полином $f(x)$ нема реалних нула. Ако он не би био нерастављив, онда и његови фактори $g(x)$ и $h(x)$ такође не би имали реалних нула. Стога су они истог знака за све реалне вредности промењиве. Не умањујући општост разматрања, можемо претпоставити да је $g(x) > 0$ и $h(x) > 0$ за све реалне вредности x. Како је $f(a_k) = 1$, следи да је $g(a_k) = h(a_k) = 1$ за свако $k = 1,2, \dots, n$. Ако је степен полинома $g(x)$ или $h(x)$ мањи од n, тада је полином $g(x)$ или $h(x)$ идентички једнак јединици, што је у контрадикцији са претпоставком да је полином $f(x)$ растављив. Остаје да се размотри могућност када је $d^\circ g(x) = d^\circ h(x) = n$. Како је $g(a_k) = h(a_k) = 1$ за свако $k = 1,2, \dots, n$ и $d^\circ g(x) = d^\circ h(x) = n$, полиноме $g(x)$ и $h(x)$ можемо представити у облику:

$$g(x) = \alpha(x - a_1)(x - a_2) \cdot \dots \cdot (x - a_n) + 1$$

$$h(x) = \beta(x - a_1)(x - a_2) \cdot \dots \cdot (x - a_n) + 1,$$

где су α и β неки цели бројеви. Како је $f(x) = g(x)h(x)$, следи да је:

$$(x - a_1)^2(x - a_2)^2 \cdot \dots \cdot (x - a_n)^2 + 1$$
$$= \alpha\beta(x - a_1)^2 \cdot \dots \cdot (x - a_n)^2 + (\alpha + \beta)(x - a_1) \cdot \dots \cdot (x - a_n) + 1$$

Изједначавањем коефицијената уз степене x^{2n} и x^n добијамо следећи систем једначина:

$$\alpha\beta = 1$$

$$\alpha + \beta = 0.$$

Овај систем једначина нема целобројна решења, што је у контрадикцији са чињеницом да су α и β цели бројеви. Тиме смо доказали да је полином $f(x)$ нерастављив.

6. Нерастављивост по модулу p

Нека је $\mathbb{Z}_p$ поље остатка по модулу p. Сваки полином са целобројним коефицијентима може се посматрати као полином са коефицијентима из поља $\mathbb{Z}_p$. Полином који је

нерастављив над $\mathbb{Z}$ може бити растављив над $\mathbb{Z}_p$, за свако p, што нам показује следећа теорема.

Теорема 6.1. Полином $q(x) = x^4 + ax^2 + b^2$, $a, b \in \mathbb{Z}$, је растављив над $\mathbb{Z}_p$ за сваки природан број p.

Доказ: За $p = 2$ постоје само 4 полинома која можемо да посматрамо и то:

$$x^4, \qquad x^4 + x^2 = x^2(x^2 + 1), \qquad x^4 + 1 = (x + 1)^4, \qquad x^4 + x^2 + 1 = (x^2 + x + 1)^2.$$

Сваки од ових полинома је растављив.

Нека је p непаран природан број. Тада можемо да изаберемо цео број s такав да је $a \equiv 2s \pmod{p}$. Дакле, имамо:

$$q(x) = x^4 + ax^2 + b^2 \equiv (x^2 + s)^2 - (s^2 - b^2) \equiv$$

$$\equiv (x^2 + b)^2 - (2b - 2s)x^2 \equiv$$

$$\equiv (x^2 - b)^2 - (-2b - 2s)x^2 \pmod{p}.$$

Да бисмо доказ завршили довољно је да докажемо да је један од бројева $s^2 - b^2, 2b - 2s, -2b - 2s$ квадратни остатак при модулу p.

Претпоставимо да $2b - 2s$ и $-2b - 2s$ нису квадрати по модулу p. Како је $(2b - 2s)(-2b - 2s) = 4(s^2 - b^2)$, довољно је доказати да је њихов производ квадрат по модулу p.

Нека је $f(x) = x^2$. Тада се x и $-x$ са $f(x)$ сликају у исти елемент. Самим тим слика целог скупа ненула елемената из $\mathbb{Z}_p$ има $\frac{p-1}{2}$ елемената. Насупрот томе, ако је $x = y^2$ онда је $x^{\frac{p-1}{2}} = y^{p-1} = 1$, то јест, све слике елемената, којих има $\frac{p-1}{2}$, задовољавају једнакост $x^{\frac{p-1}{2}} = 1$, која нема више од $\frac{p-1}{2}$ решења. Елементи који нису слика функције $f(x)$ задовољавају једнакост $x^{\frac{p-1}{2}} = -1$. Сходно томе, ако два цела броја нису потпун квадрат по модулу p, онда је њихов производ потпун квадрат по модулу p.

7. Библиографија

Димитријевић, 2011: Радослав Димитријевић, *Збирка задатака из теорије полинома*, Београд, ДМС

Ђукић: Душан Ђукић, *Полиноми по једној променљивој*, дигитално издање

Калајџић, 2008: Гојко Калајџић, *Алгебра*, Београд, Математички факултет

Прасолов, 2001: Виктор В. Прасолов, *Полиноми*, Москва, Московски центар за континуирану математику