Zapiski pri predmetu Proseminar B [1]

Emil Žagar

29. marec 2013

[1]Skripta je v nastajanju, zato je gotovo polna napak. Hvaležen bom za vse pripombe. Iskanje napak je obenem del učnega procesa pri Proseminarju B.

Kazalo

1 Nekaj dokazov o neskončnosti praštevil **5**
1.1 Formalna definicija naravnih števil 5
1.2 Relacije in osnovne algebrske strukture 6
1.2.1 Deljivost v kolobarju celih števil 9
1.2.2 Lagrangeev izrek za končne grupe 10
1.3 Prvi dokaz 11
1.4 Drugi dokaz 12
1.5 Tretji dokaz 12
1.6 Četrti dokaz 13
1.7 Peti dokaz 15
1.8 Šesti dokaz 18
1.9 Sedmi dokaz 19
1.10 Osmi dokaz 19
1.11 Nekaj odprtih problemov, povezanih s praštevili 20
1.11.1 Praštevilski dvojčki 20
1.11.2 Mersennova praštevila 22
1.11.3 Fermatova praštevila 23
1.12 Porazdelitev praštevil 24

2 Polinomi in njihove ničle **31**
2.1 Uvod 31
2.2 Formalna konstrukcija polinomov 31
2.3 Evklidov algoritem 33
2.4 Ničle polinomov 36

3 Kompleksni polinomi **39**
3.1 Osnovni izrek algebre 39
3.2 Descartesovo pravilo predznakov 43
3.3 Meje za ničle kompleksnega polinoma 50

Poglavje 1

Nekaj dokazov o neskončnosti praštevil

1.1 Formalna definicija naravnih števil

Naravna števila poznamo že od malih nog. Govorili so nam, da so naravna števila tista, "s katerimi štejemo". Ponavadi naravna števila označimo s simbolom $\mathbb{N}$, elemente pa zaporedoma s števili 1, 2,... Torej je $\mathbb{N} = \{1, 2, 3, \dots\}$. Matematiki se s tako razlago ne zadovoljimo. Zanima nas, ali lahko naravna števila postavimo na trdnejše temelje. Oglejmo si, kako.

Definicija 1.1. *Množica naravnih števil* $\mathbb{N}$ *je vsaka množica, ki zadošča naslednjim Peanovim aksiomom:*

A1. Množica $\mathbb{N}$ *vsebuje odlikovani element* e.

A2. Vsak element $n \in \mathbb{N}$ *ima natančno določenega naslednika* $s(n) \in \mathbb{N}$.

A3. Element e *ni naslednik nobenega elementa iz* $\mathbb{N}$.

A4. Za poljubna elementa $m, n \in \mathbb{N}$ *velja, da iz* $s(m) = s(n)$ *sledi* $m = n$.

A5. Naj bo M *taka podmnožica množice* $\mathbb{N}$*, da je*

a) $e \in M$,

b) Če je $m \in M$*, potem je tudi* $s(m) \in M$.

Potem je $M = \mathbb{N}$.

Primer 1.1. *Standardna reprezentacija naravnih števil* $\mathbb{N}$ *je množica* $\mathbb{N} = \{1, 2, 3, \dots\}$*, pri čemer je* $s(m) = m + 1$.

V prejšnjem primeru smo tiho privzeli operacijo seštevanja. Tudi to lahko uvedemo zelo formalno.

Definicija 1.2. *Standardno seštevanje $+$ na množici naravnih števil $\mathbb{N}$ je predpis $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, za katerega velja:*

a) $n + 1 = s(n), \quad n \in \mathbb{N}$,

b) $m + s(n) = s(m + n), \quad m, n \in \mathbb{N}$.

Primer 1.2. *Naravna števila lahko reprezentiramo tudi z množico*

$$\mathbb{N} = \{1, 2^1, 2^2, 2^3, \dots\},$$

na njej pa definiramo "seštevanje" $\oplus$ kot $2^m \oplus 2^n = 2^{m+n}$, kjer je v eksponentu standardno seštevanje.

Od sedaj naprej bomo na množico $\mathbb{N}$ gledali kot na standardno množico $\mathbb{N} = \{1, 2, 3, \dots\}$, na kateri je definirano standardno seštevanje. Da bi o naravnih številih lahko povedali še kaj več, jih bomo najprej umestili v razširjeno množico celih števil z bogatejšo strukturo.

1.2 Relacije in osnovne algebrske strukture

V tem poglavju bomo definirali pojem relacije in nekaj algebrskih struktur, ki jih bomo potrebovali kasneje. Podrobno teorijo o alebrskih strukturah lahko bralec najde denimo v učbeniku [8]. Začnimo s pojmom relacije. Denimo, da je dana neprazna množica A.

Definicija 1.3. *Relacija R na neprazni množici A je podmnožica kartezičnega produkta $A \times A$.*

Pravimo, da je par elementov $a, b \in A$ v relaciji R, če $(a, b) \in R$. Na kratko pišemo $a\,R\,b$. Relacije so lahko zelo splošne, odvisno od tega, kakšna je množica A in kakšna je lastnost, ki določa relacijo.

Primer 1.3. *Naj bo A množica učencev na šoli. Relacija je denimo lahko pripadnost istemu razredu. Natančneje, učenca a in b sta v relaciji R, če sta v istem razredu.*

Relacije imajo lahko različne lastnosti, od katerih so med najbolj pomembnimi naslednje tri:

- Relacija je *refleksivna*, če je $a\,R\,a$ za vsak $a \in A$.

- Relacija je *simetrična*, če iz $a\,R\,b$ sledi $b\,A\,a$, za vsak par $a, b \in A$.
- Relacija je *Tranzitivna*, če $a\,R\,b$ in $b\,R\,c$ sledi $a\,R\,c$ za vsako trojico $a, b, c \in A$.

Definicija 1.4. *Relaciji R, ki je refleksivna, simetrična in tranzitivna, rečemo ekvivalenčna relacija. Tedaj elementoma, ki sta v relaciji R, rečemo, da sta ekvivalentna. Množico vseh elementov, ki so v relaciji R z elementom $a \in A$, imenujemo ekvivalenčni razred R_a s predstavnikom a.*

Brez dokaza podajmo naslednji pomembni izrek o ekvivalenčnih relacijah.

Izrek 1.1. *Ekvivalenčna relacija R razdeli množico A na same med seboj disjunktne razrede. Dva elementa pripadata istemu rezredu, če sta ekvivalentna, različnima razredoma pa, če nista ekvivalentna.*

Relacija iz prejšnjega primera je ekvivalenčna (preverite). Ekvivalenčni razredi dobesedno šolski razredi.
Relacije imajo lahko še veliko drugih pomembnih lastnosti, vendar bo za našo nadaljnjo obravnavo dovolj poznati ekvivalenčne relacije.

Posvetimo se sedaj nekaterim algebrskih strukturam. Začnimo z definicijo notranje binarne operacije.

Definicija 1.5. *Notranja binarna operacija na neprazni množici A je vsaka preslikava $\circ : A \times A \to A$, ki vsakemu paru elementov $a, b \in A$ priredi natanko določen element $c \in A$. To ponavadi zapišemo takole*

$$a \circ b = c.$$

Množici A, opremljeni z notranjo operacijo, rečemo grupoid.
Element $e \in A$ je v grupoidu leva enota (levi nevtralni element), če je $e \circ x = x$ za vsak $x \in A$. Podobno je e desna enota (desni nevtralni element), če je $x \circ e = x$ za vsak $x \in A$. Če je element hkrati leva in desna enota ga imenujemo enota ali nevtralni element.
V grupoidu z enoto e je element $a' \in A$ je levi inverzni element k $a \in A$, če je $a' \circ a = e$. Podobno je $a' \in A$ desni inverzni element k elementu a, če je $a \circ a' = e$. Če pa za element $a' \in A$ velja, da je $a' \circ a = a \circ a' = e$, je a' inverzni element k elementu a. Elementu a tedaj rečemo, da je obrnljiv element.

Pogosto grupoid označimo kot urejen par $(A, \circ)$.

Primer 1.4. *Primer grupoida je denimo prostor vseh trirazsežnih vektorjev z operacijo vektorskega produkta.*

Definicija 1.6. *Če je v grupoidu $(A, \circ)$ operacija $\circ$ asociativna, torej, če za vsako trojico elementov $a, b, c \in A$ velja*

$$(a \circ b) \circ c = a \circ (b \circ c),$$

potem grupoidu rečemo polgrupa ali monoid.

Primer 1.5. *Primer polgrupe so denimo naravna števila za operacijo seštevanja. Če naravnim številom dodamo še ničlo, torej, če gledamo množico $\mathbb{N}_0$, je element 0 enota grupoida $(\mathbb{N}_0, +)$, noben element pa ni obrnljiv (niti z leve, niti z desne).*
Trirazsežni vektorji z operacijo vektorskega produkta iz prejšnjega primera pa niso polgrupa (zakaj?).

Definicija 1.7. *Polgrupo $(A, \circ)$ z enoto, v kateri so vsi elementi obrnljivi, imenujemo grupa. Grupa je Abelova (ali komutativna), če je operacija $\circ$ komutativna, torej, če za vsak par $a, b \in A$ velja $a \circ b = b \circ a$. Množica $B \subseteq A$ je podgrupa grupe A, če je sama grupa glede na isto operacijo.*

Primer 1.6. *Cela števila $\mathbb{Z}$ za operacijo seštevanja so Abelova grupa. Enota je število 0, elementu $a \in \mathbb{Z}$ inverzni element pa je $-a$.*

Definicija 1.8. *Denimo, da imamo v množici A dve notranji operaciji, označimo ju $z +$ (adicija) in $\cdot$ (multiplikacija). Naj bo operacija $\cdot$ distibutivna glede na $+$, to pomeni, da za vsako trojico $x, y, z \in A$ velja*

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z),$$
$$(x + y) \cdot z = (x \cdot z) + (y \cdot z).$$

Pravimo, da je $(A, +, \cdot)$ kolobar, če je

- *$(A, +)$ Abelova grupa,*
- *$(A, \cdot)$ polgrupa,*
- *multiplikacija distributivna glede na adicijo.*

Če je multiplikacija $\cdot$ komutativna, imenujemo kolobar $(A, +, \cdot)$ komutativen. Če je $(A, \cdot)$ polgrupa z enoto, bomo to enoto označili z 1 in ga imenovali enota kolobarja. V tem primeru bomo rekli, da je $(A, +, \cdot)$ kolobar z enoto.

Primer 1.7. *Primer komutativnega kolobarja z enoto je kolobar $(\mathbb{Z}, +, \cdot)$, kjer sta $+$ in $\cdot$ običajno seštevanje in množenje celih števil.*

Definicija 1.9. *Če v kolobarju $(A, +, \cdot)$ za elementa $a, b \neq 0$, kjer je 0 enota v Abelovi grupi $(A, +)$, velja, da je $a \cdot b = 0$, je a levi, b pa desni deliteljniča. Kolobar, ki nima deliteljev niča, se imenuje kolobar brez deliteljev niča.*

Primer 1.8. *Kolobar ostankov pri deljenju s 4, na kratko $\mathbb{Z}_4$, je primer kolobarja, ki ima delitelje niča. Katere?*

Definicija 1.10. *Komutativnemu kolobarju z enoto in brez deliteljev niča rečemo celostno polje.*

Definicija 1.11. *Kolobar $(A, +, \cdot)$ z enoto je obseg natanko tedaj, ko so vsi neničelni elementi (torej tisti, ki niso enaki enoti za aditivno grupo $(A, +)$), obrnljivi. Obseg je komutativen, če je kolobar komutativen. Takemu obsegu rečemo polje.*

Primer 1.9. *Primer komutativnega obsega so realna števila $\mathbb{R}$ za običajno seštevanje in množenje.*

V naslednjem podrazdelku bomo podrobneje spoznali nekaj lastnosti posebnega kolobarja, kolobraja celih števil

1.2.1 Deljivost v kolobarju celih števil

Posvetimo se torej kolobarju $(\mathbb{Z}, +, \cdot)$, kjer je $\mathbb{Z}$ množica celih števil $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, $+$ običajno se'stevanje, $\cdot$ pa običajno množenje. Zlahka se prepričamo, da je množica $\mathbb{Z}$ z omenjenima operacijama res kolobar. V resnici je kolobar z enoto (enota je element 1) brez deliteljev niča, torej celostno polje. Oglejmo si nekaj osnovnih lastnosti, ki sledijo iz te strukture.

Definicija 1.12. *Za celi števili $m, n \in \mathbb{Z}$ pravimo, da m deli n (oziroma, da je n deljivo z m), če obstaja tako celo število $k \in \mathbb{Z}$, da je $n = k\,m$. Številu m rečemo tudi delitelj števila n.*

Neposredno na deljivost se nanaša naslednji pomembni izrek.

Izrek 1.2. *Naj bo $a, b \in \mathbb{Z}$, $b \neq 0$. Potem obstajata enolično določeni celi števili q in r, da je*

$$a = q\,b + r, \quad 0 \leq r < |b|.$$

Dokaz. Izrek bomo dokazali samo za nenegativno število a in pozitivno število b. Dokazi ostalih primerov so podobni.
Definirajmo množico $S = \{x \in \mathbb{Z};\ x = a - z\,b,\ z \in \mathbb{Z},\ x \geq 0\}$. Množica S je neprazna, saj vsebuje vsaj element a. Ker je navzdol omejena z 0,

vsebuje najmanjši element, denimo r. Potem seveda obstaja tak $q \in \mathbb{Z}$, da je $r = a - q\,b$, oziroma $a = q\,b + r$. Izrek bo dokazan, če utemeljimo zvezo $0 \leq r < b$.
Ker je $r \in S$, je $r \geq 0$. Privzemimo, da je $r \geq b$. Potem je $0 \leq r - b < r$, saj je $b > 0$. Torej je

$$r - b = (a - q\,b) - b = a - b\,(q + 1).$$

Iz definicije množice S sledi, da je $r - b \in S$, kar je v protislovju z dejstvom, da je r najmanjši element množice S. □

Za poljubni dve števili, ki nimata nobenega skupnega delitelja razen 1, pravimo, da sta tuji. Primer para tujih števil sta denimo 15 in 22.
Množica naravnih števil $\mathbb{N}$ je prava podmnožica celih števil $\mathbb{Z}$. Videli smo že, da ima strukturo monoida. Sedaj, ko poznamo pojem deljivosti, lahko nekatera naravna števila posebej odlikujemo.

Definicija 1.13. *Naravno število $n > 1$ je praštevilo, če je deljivo samo z ena in samim seboj. Naravnemu številu, ki ni praštevilo, rečemo sestavljeno število.*

Praštevila gotovo že poznamo. Edino sodo praštevilo je 2, nekaj prvih praštevil pa je 2, 3, 5, 7, 11, ... Množico praštevil bomo označili s $\mathbb{P}$. Prvo sestavljeno število pa je 4, saj je $4 = 2 \cdot \cdots 2$. Zelo pomemben je naslednji izrek.

Izrek 1.3. *Vsako sestavljeno število n je produkt dveh števil, ki sta strogo med 1 ter n in ima vsaj enega praštevilskega delitelja.*

Od tod lahko izpeljemo pomemben izrek o razcepu naravnega števila na produkt praštevil (prafaktorjev).

Izrek 1.4. *Vsako naravno število $n > 1$ lahko zapišemo kot produkt praštevil do vrstnega reda natančno.*

Dokaza obeh zgornjih izrekov lahko bralec najde na primer v [2].

1.2.2 Lagrangeev izrek za končne grupe

Ena od pomembnih lastnosti nekaterih elementov v grupi $(A, \circ)$ je *red elementa*.

Definicija 1.14. *Red elementa a grupe $(A, \circ)$ z enoto e je najmanjše naravno število n, za katerega je $a^n = e$. Če tako število ne obstaja, pravimo, da je red elementa a neskončno. Pri tem je $a^n = \underbrace{a \circ a \circ \cdots \circ a}_{n-\text{krat}}$.*

Dokaj očitno je, da imajo vsi elementi končne grupe končen red. V neskončnih grupah to ni nujno res. Element $(-1) \in \mathbb{R}$ v multiplikativni grupi $(\mathbb{R}\backslash\{0\}, \cdot)$ ima red 2, medtem, ko element 2 nima končnega reda.

PRIMER 1.10. *Vzemimo multiplikativno grupo ostankov* $\mathbb{Z}_7' = \{1, 2, 3, \ldots, 6\}$. *Hitro se prepričamo, da imajo elementi zaporedoma red enak* 1, 3, 6, 3, 6 *in* 2. *Opazimo, da red vsakega elementa deli* 6, *moč grupe* $\mathbb{Z}_7'$.

Opazka iz prejšnjega primera velja splošno za končne grupe (take, ki imajo končno mnogo elementov).

IZREK 1.5. *Naj bo* $(A, \circ)$ *končna grupa in* B *njena podgrupa. Potem moč grupe* B *deli moč grupe* A. *Za vsak element* $a \in A$ *z redom* r *velja, da* r *deli moč grupe* A.

DOKAZ. Označimo z $|A|$ in $|B|$ zaporedoma moč grupe A in moč podgrupe B. Definirajmo relacijo R na A takole: elementa $a, b \in A$ sta v relaciji R natanko tedaj, ko $b \circ a^{-1} \in B$.
Ker je B podgrupa in $a \circ a^{-1} = e \in B$, je R refleksivna. Če izberemo tak par $a, b \in A$, da je $b \circ a^{-1} \in B$, je tudi $(b \circ a{-}1)^{-1} = a \circ b^{-1} \in B$ in je zato R simetrična. Izberimo sedaj take elemente $a, b, c \in A$, da je $a\,R\,b$ in $b\,R\,c$. Torej je $b \circ a^{-1}, c \circ b^{-1} \in B$. Ker je B podgrupa, je tudi $(c \circ b^{-1}) \circ (b \circ a^{-1}) = c \circ a^{-1} \in B$, zato je $a\,R\,c$ in relacija R je tranzitivna. Dokazali smo torej, da je R ekvivalenčna relacija.
Ekvivalenčni razred, ki vsebuje nek element $a \in A$, je natanko množica

$$B \circ a := \{x \circ a;\ x \in B\}\,,$$

t.i. desni odsek po podgrupi B. Očitno je $|B|$ enako $|B \circ a|$. Vemo tudi, da grupa A razpade na disjuktne ekvivalenčne razrede glede na relacijo R. Zato je $|A| = k\ |B|$, $k \in \mathbb{N}$, torej moč podgrupe B deli moč grupe A.
Dokažimo še drugi del izreka. Naj bo $a \in A$ in njegov red r. Množica

$$C = \left\{a, a^2, a^3, \ldots, a^r\right\}$$

je ciklična podgrupa grupe A. Njena moč je r, zato po prej dokazanem r deli $|A|$, kar smo želeli dokazati. □

1.3 Prvi dokaz

Oglejmo si sedaj prvi dokaz o neskončnosti praštevil. Znan je kot Evklidov dokaz in temelji na preprostem premisleku o deljivosti naravnih števil.

Predpostavimo torej, da je množica $\mathbb{P} = \{2, 3, 5, 7, 11 \dots\}$ končna. Obstaja torej končno mnogo praštevil p_1, p_2, $\dots$,p_n, $n \in \mathbb{N}$. Oglejmo si število

$$q = \prod_{k=1}^{n} p_k + 1 = p_1\, p_2 \cdots p_n + 1.$$

Število q je gotovo večje od vsakega izmed števil p_k, $k = 1, 2, \dots, n$, zato po predpostavki ne more biti praštevilo. Torej je sestavljeno število. Toda vsako sestavljeno število je po izreku 1.3 deljivo z nekim praštevilom. To pomeni, da je $q = r\, p_i$, $r \in \mathbb{N}$, $i \in \{1, 2, \dots, n\}$. Toda p_i deli q in $p_1\, p_2 \cdots p_n$, torej tudi $q - p_1\, p_2 \cdots p_n = 1$, kar ni mogoče.

1.4 Drugi dokaz

V prejšnjih poglavjih smo si nabrali dovolj znanja iz teorije grup, da si lahko ogledamo še drugi dokaz o neskončnosti množice praštevil $\mathbb{P}$. Predpostavimo spet, da je množica $\mathbb{P}$ končna in p največje praštevilo v njej. Oglejmo si t.i. *Mersenneovo število* $\hat{p} = 2^p - 1$. Dokazali bomo, da je vsak praštevilski faktor števila $\hat{p}$ večji od p, kar je v prostislovju s končnostjo množice $\mathbb{P}$.
Naj bo q praštevilo, ki deli $\hat{p}$ (tako število po izreku 1.3 gotovo obstaja). Ker je p praštevilo, ima element 2 red p v multiplikativni grupi $\mathbb{Z}_q^{'}$. Red namreč ne more biti manjši, saj bi sicer delil p, kar ni mogoče, ker je p praštevilo. Grupa $\mathbb{Z}_q^{'}$ ima $q - 1$ elementov, zato po Lagrangeevem izreku p deli $q - 1$, kar pomeni, da je $q > p$.

1.5 Tretji dokaz

V tem dokazu bomo uporabili znana *Fermatova števila*

$$F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, \dots$$

Dokazali bomo, da sta poljubini dve različni Fematovi števili tuji. (Prepričajte se, da od tod sledi, da mora biti praštevil neskončno mnogo.) Najprej dokažimo naslednjo lemo.

Lema 1.1. *Za Fermatova števila velja naslednja rekurzijska zveza*

$$\prod_{k=0}^{n-1} F_k = F_n - 2, \quad n = 1, 2, \dots$$

Dokaz. Zvezo bomo dokazali z indukcijo. Za $n = 1$ je očitno res $F_0 = F_1 - 2$. Privzemimo sedaj, da zveza velja za neko naravno število $n \in \mathbb{N}$. Od tod moramo izpeljati veljavnost zveza za $n + 1$. Računajmo

$$\prod_{k=0}^{n} F_k = \left(\prod_{k=0}^{n-1} F_k\right) F_n = (F_n - 2)\, F_n = \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) = 2^{2^{n+1}} - 1$$
$$= F_{n+1} - 2.$$

□

Naj bo sedaj število $m > 1$ delitelj dveh Fermatovih števiil F_k in F_ℓ, $k < \ell$. Po pravkar dokazani lemi m deli 2, torej je $m = 1$ ali $m = 2$. Prvo možnost smo izločili s predpostavko, druga pa odpade, ker so vsa Fermatova števila liha.
Opomnimo, da je v zgodovini nekaj časa veljala zmota, da so Fermatova števila praštevila. Od tod bi neposredno sledilo, da je praštevil neskončno mnogo. Z računalniko se dandanes hitro prepričamo, da prva štiri Fermatova števila res praštevila, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ in $F_4 = 65537$. Peto Fermatovo število pa je sestavljeno, $F_5 = 4294967297 = 641 \cdot 6700417$. Dandanes ni znano, ali je poleg F_i, $i = 1, 2, 3, 4$, še kakšno Fermatovo število praštevilo.

1.6 Četrti dokaz

Naslednji dokaz temelji mnogo bolj na analizi, kot prejšnji. Označimo z

$$\pi(x) := \#\left\{p \le x;\, p \in \mathbb{P}\right\},$$

torej število praštevil, ki so manjša od (realnega) števila x. Uredimo praštevila v množici $\mathbb{P}$ naraščajoče, torej $\mathbb{P} = \{p_1, p_2, p_3, \dots\}$, kjer je $p_1 < p_2 < p_3 < \cdots$ Funkcijo log definirajmo z integralom

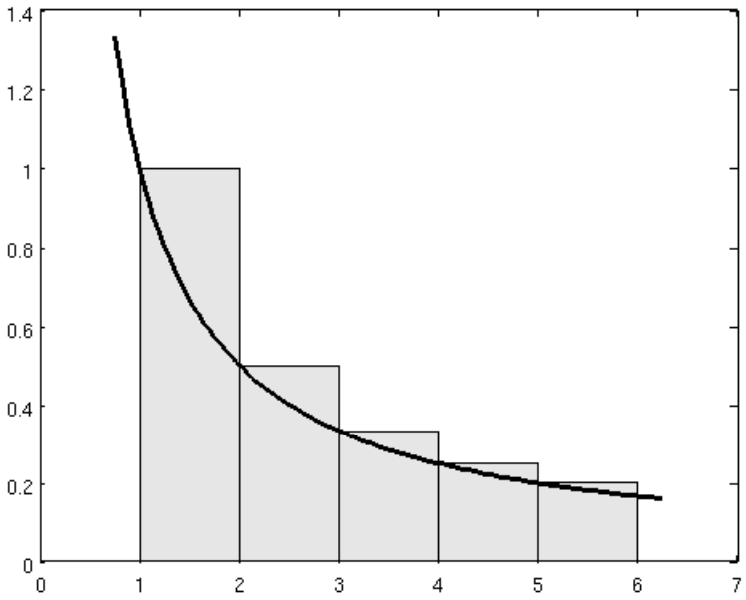
$$\log x = \int_1^x \frac{1}{t}\,\mathrm{d}t.$$

Če primerjamo ploščino pod grafom funkcije $f(x) = 1/x$ z njeno zgornjo Riemannovo vsoto (glejte sliko 1.1), potem opazimo, da za $n \le x < n + 1$ velja

$$\log x \le 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1} + \frac{1}{n} =: H_n. \tag{1.1}$$

Očitno je

$$H_n \le \sum_{m \in \mathcal{M}} \frac{1}{m}, \tag{1.2}$$



Slika 1.1: Zgornja Riemannova vsota (ploščina senčenega lika) funkcije $f(x) = 1/x$ na intervalu $[1, 6]$.

kjer je $\mathcal{M} \subset \mathbb{N}$ množica vseh takih naravnih števil, ki imajo samo praštevilske delitelje manjše ali enake x. Vsako število $m \in \mathcal{M}$ lahko po izreku 1.4 enolično (do vrstnega reda faktorjev) zapišemo kot

$$m = \prod_{p \in \mathbb{P},\ p \leq x} p^{e_p}, \quad e_p \in \mathbb{N}.$$

Od tod hitro vidimo, da je

$$\sum_{m \in \mathcal{M}} \frac{1}{m} = \prod_{p \in \mathbb{P}, p \leq x} \left(\sum_{k=0}^{\infty} \frac{1}{p^k} \right). \tag{1.3}$$

Vsota v (1.3) je geometrijska vrsta s kvocientom $1/p$, kar skupaj z (1.1) in (1.2) da

$$\log x \leq \prod_{p \in \mathbb{P}, p \leq x} \frac{1}{1 - \frac{1}{p}} = \prod_{p \in \mathbb{P}, p \leq x} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}.$$

Ker so števila p_k urejena po velikosti, zlahka (denimo z indukcijo) dokažemo, da je $p_k \geq k+1$, $k = 1, 2, \ldots$ Torej je

$$\frac{p_k}{p_k - 1} = 1 + \frac{1}{p_k - 1} \leq 1 + \frac{1}{k} = \frac{k+1}{k}$$

in zato

$$\log x \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1.$$

Funkcija log raste čez vse meje, zato po zgornji neenakosti tako raste tudi funkcija π. Torej je praštevil neskončno mnogo, kar smo želeli dokazati.

1.7 Peti dokaz

V prejšnjih dokazih smo dodobra uporabili teorijo števil, algebro in analizo. Naslednji dokaz pa sloni na popolnoma drugih temeljih, na topologiji. Bralec lahko veliko o topologiji izve denimo v knjigi [5]. Začnimo z definicijo.

Definicija 1.15. *Naj bo X neka množica in τ družina podmnožic množice X, torej $\tau \subset \mathcal{P}(X)$, kjer je $\mathcal{P}(X)$ potenčna množica množice X. Družina τ je topologija na X, če velja:*

1. *Prazna množica in množica X sta elementa τ.*
2. *Poljubna unija množic iz τ je v τ.*

3. Vsak presek končno mnogo množic iz τ je v τ.

Paru (X, τ), ki zadošča pogojem iz prejšnje definicije rečemo topološki prostor, množicam iz τ pa odprte množice. Množicam, katerih komplementi so odprte množice, torej v τ, rečemo zaprte množice.

PRIMER 1.11. *Naj bo $X = \{1, 2, 3, 4\}$. Primeri topologij na X so:*

- *Trivialna topologija: $\tau = \{\{\}, X\}$.*
- *Diskretna topologija: $\tau = \mathcal{P}(X)$.*
- $\tau = \{\{\}, \{2\}, \{1, 2\}, \{2, 3\}, \{1, 2, 3\}, \{1, 2, 3, 4\}\}$.

PRIMER 1.12. *Naj bo $X = \mathbb{Z}$ in τ množica vseh končnih podmnožic $\mathbb{Z}$ ter $\mathbb{Z}$. Prepričajte se, da τ ni topologija.*
Namig: oglejte si denimo unijo vseh končnih podmnožic $\mathbb{Z}$, ki ne vsebujejo elementa 0.

PRIMER 1.13. *Naj bo $X = \mathbb{R}$. Množica τ naj bo sestavljena iz vseh množic $U \subseteq \mathbb{R}$, za katere velja: za vsak element $u \in U$ obstaja $r > 0$, da je $(u - r, u + r) \subseteq U$. Prepričajte se, da je τ topologija na $\mathbb{R}$.*

Oglejmo si sedaj posebno topologijo. Vzemimo $X = \mathbb{Z}$. Za izbrani celi števili a in $b > 0$ naj bo

$$N_{a,b} := \{a + n\, b;\ n \in \mathbb{Z}\}\,.$$

Vsaka množica $N_{a,b}$ je torej bineskončno aritmetično zaporedje. Rekli bomo, da je množica $U \subseteq \mathbb{Z}$ odprta, če je bodisi prazna, bodisi za vsak $a \in U$ obstaja $b > 0$, da je $N_{a,b} \subseteq U$.

LEMA 1.2. *Zgornja definicija odprtih množic poraja topologijo na $\mathbb{Z}$.*

DOKAZ. Prazna množica je po definiciji odprta. Izberimo poljubno število $a \in \mathbb{Z}$. Potem je množica $N_{a,1} = \mathbb{Z} \subseteq \mathbb{Z}$, zato je $\mathbb{Z}$ odprta.
Vzemimo sedaj unijo odprtih množic U_λ, $\lambda \in \Lambda$, torej

$$U = \bigcup_{\lambda \in \Lambda} U_\lambda.$$

Naj bo $a \in U$. Potem obstaja tak $\lambda_0 \in \Lambda$, da je $a \in U_{\lambda_0}$. Ker je U_{λ_0} odprta, obstaja tak $b > 0$, da je $N_{a,b} \subseteq U_{\lambda_0}$. Toda potem je $N_{a,b} \subseteq U$ in zato je U odprta.
Naj bosta sedaj U_1 in U_2 odprti množici. Dokazati moramo, da je tudi njun

pesek odprta množica. Če je presek prazen, ni kaj dokazovati. Predpostavimo, da je $U = U_1 \cap U_2 \neq \emptyset$. Izberimo $a \in U$. Torej je $a \in U_1$ in $a \in U_2$. Zato obstajata taki števili $b_1, b_2 > 0$, da je $N_{a,b_1} \subseteq U_1$ in $N_{a,b_2} \subseteq U_2$. Toda potem je množica $N_{a,b_1\,b_2} \subseteq U_1 \cap U_2$, zato je U odprta množica, kar smo želeli dokazati. □

Dokažimo še naslednjo lemo.

LEMA 1.3. *Vsaka neprazna odprta množica je neskončna in vsaka množica $N_{a,b}$ je tudi zaprta.*

DOKAZ. Prvi del trditve sledi iz definicije odprte množice. Za dokaz drugega dela pa preverimo, da je

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}.$$

Izberimo $c \in N_{a,b}$. Torej je $c = a + n\,b$, za neko celo število n. Če je $c \in \bigcup_{i=1}^{b-1} N_{a+i,b}$, mora biti $c = a+i+n_i\,b$, kjer je $n_i \in \mathbb{Z}$, za nek $i \in \{1, 2, \ldots, b-1\}$. Torej je $i = (n - n_i)\,b$. Ker $n - n_i \neq 0$, mora biti i deljiv z b, kar ni mogoče, saj je $1 \leq i \leq b - 1$. To dokazuje inkluzijo

$$N_{a,b} \subseteq \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}. \tag{1.4}$$

Izberimo sedaj $c \in ZZ \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}$. Torej c ne more biti oblike

$$c = a + i + n_i\,b, \quad i = 1, 2, \ldots b - 1. \tag{1.5}$$

Toda $c - a$ se da po izreku 1.2 enolično zapisati v obliki $c - a = q\,b + r$, $q, r \in \mathbb{Z}$, $0 \leq r < b$. Zaradi (1.5), ostane samo možnost $c - a = q\,b$, torej je $c \in N_{a,b}$, kar pomeni, da je $\mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b} \subseteq N_{a,b}$. Skupaj z (1.4) dobimo $N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}$ in lema je dokazana. □

Do sedaj v dokazu praštevil še omenili nismo. Pa jih dajmo. Vemo, da ima vsako število $n \neq 1, -1$ praštevilskega delitelja. Zato je torej tako število vsebovano v množici $N_{0,p}$. Od tod sledi, da je

$$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}.$$

Denimo, da je množica $\mathbb{P}$ končna. Potem je po definiciji topologije množica $\bigcup_{p\in\mathbb{P}} N_{0,p}$ zaprta, saj je končna unija zaprtih množic. Torej je množica $\{-1, 1\}$ odprta, kar je v nasprotju z dejstvom, da je vsaka neprazna odprta množica neskončna.

1.8 Šesti dokaz

V tem dokazu poleg neskončnosti praštevil dokažemo še zanimivo dejstvo, da vrsta

$$\sum_{p\in\mathbb{P}} \frac{1}{p} \tag{1.6}$$

divergira. Prvi je to dokazal že Euler, v tem dokazu pa uporabimo ideje Erdösa.

Ponovno zapišimo vsa praštevila v naraščajočem vrstnem redu, torej $p_1, p_2, p_3, \ldots$. Privzemimo, da vrsta (1.6) konvergira. Potem obstaja tako naravno število k, da je

$$\sum_{i\geq k+1} \frac{1}{p_i} < \frac{1}{2}. \tag{1.7}$$

Poimenujmo praštevila $p_1, p_2, \ldots, p_k$ "majhna praštevila" in $p_{k+1}, p_{k+2}, \ldots$ "velika" praštevila. Za vsako naravno število N iz (1.7) sledi

$$\sum_{i\geq k+1} \frac{N}{p_i} < \frac{N}{2}. \tag{1.8}$$

Označimo z N_b število tistih naravnih števil $n \leq N$, ki so deljiva z vsaj enim velikim praštevilom, in z N_s število tistih naravnih števil $n \leq N$, ki imajo samo majhne praštevilske delitelje. Pokazali bomo, da obstaja tako naravno število N, za katerega je

$$N_b + N_s < N.$$

To je seveda v prostislovju z očitnim dejstvom $N_b + N_s = N$.
Zlahka se prepričamo, da je $\lfloor N/p_i \rfloor$ število večkratnikov števila p_i, ki so manjši ali enaki N. Torej iz (1.8) sledi

$$N_b \leq \sum_{i\geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor < \frac{N}{2}. \tag{1.9}$$

Posvetimo se sedaj številu N_s. Zapišimo število $n \leq N$ v obliki $n = a_n\, b_n^2$, kjer a_n ne vsebuje nobenega kvadrata naravnega števila. Torej je vsako število a_n produkt samih različnih majhnih praštevil. Od tod sledi, da je natanko 2^k različnih možnih faktorjev a_n. Očitno je $b \leq \sqrt{n} \leq \sqrt{N}$, je torej največ $\sqrt{N}$ možnih faktorjev b_n. Od tod očitno sledi

$$N_s \leq 2^k \sqrt{N}.$$

Naj bo sedaj $N = 2^{2k+2}$. Potem iz zgornje neenakosti sledi $N_s \leq N/2$. Skupaj z (1.9) tako dobimo protislovje $N_b + N_s < N/2 + N/2 = N$.

1.9 Sedmi dokaz

Oglejmo si še en kratek novejši dokaz o neskončnosti praštevil. Najdemo ga v [7].
Najprej dokažimo naslednjo preprosto lemo.

LEMA 1.4. *Naj bo $n \in \mathbb{N}$, $n > 1$. Potem sta števili n in $n+1$ tuji.*

DOKAZ. Denimo, da imata n in $n+1$ skupni delitelj $d > 1$. Potem je $n = d\,k_1$ in $n+1 = d\,k_2$. Razlika $n+1-n = 1 = d\,(k_2 - k_1)$ je deljiva z d, kar je nemogoče. □

Po zgornji lemi ima torej število $n(n+1)$ vsaj dva različna praštevilska delitelja. Sedaj nadaljujemo. Ker sta števil $n(n+1)$ in $n(n+1)+1$ tuji, ima produkt $n(n+1)(n(n+1)+1)$ vsaj tri različne praštevilske delitelje...

1.10 Osmi dokaz

J. P. Whang je leta 2010 podal naslednji dokaz. Naj bo $k \in \mathbb{N}$. Potem je

$$k! = \prod_{p \in \mathbb{P}} p^{f(p,k)},$$

kjer je

$$f(p,k) = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \left\lfloor \frac{k}{p^3} \right\rfloor + \cdots$$

Očitno je

$$f(p,k) < \frac{k}{p} + \frac{k}{p^2} + \frac{k}{p^3} + \cdots = \frac{k}{p-1} \leq k.$$

Torej je

$$k! = \prod_{p \in \mathbb{P}} p^{f(p,k)} < \prod_{p \in \mathbb{P}} p^k = \left(\prod_{p \in \mathbb{P}} p \right)^k,$$

od koder sledi

$$\frac{\left(\prod_{p \in \mathbb{P}} p \right)^k}{k!} > 1. \tag{1.10}$$

Če je praštevil samo končno mnogo, je

$$\lim_{k \to \infty} \frac{\left(\prod_{p \in \mathbb{P}} p \right)^k}{k!} = 0,$$

kar je v prostislovju z (1.10).

1.11 Nekaj odprtih problemov, povezanih s praštevili

1.11.1 Praštevilski dvojčki

Praštevilo p in $p+2$ pravimo praštevilska dvojčka. Primeri takih dvojčkov so $(3,5)$, $(5,7)$, $(9,11)$,... Še vedno je odprt naslednji problem.

DOMNEVA 1.1. *Praštevilskih dvojčkov je neskončno mnogo.*

Zlahka se prepričamo, da je vsak praštevilski par, razen $(3,5)$, oblike $(6\,n-1, 6\,n+1)$, $n \in \mathbb{N}$. Preden se posvetimo karakterizaciji praštevilskih dvojčkov, dokažimo pomemben Wilsonov izrek.

IZREK 1.6 (Wilsonov izrek). *Naravno število $p > 1$ je praštevilo natanko tedaj, ko je*

$$(p-1)! \equiv -1 \pmod{p}\,.$$

DOKAZ. Privzemimo, da je p praštevilo. Množica $Z_p^{'}$ je multiplikativna grupa za operacijo množenja po modulu p. Ker je množica inverznih elementov grupe $Z_p^{'}$ spet $Z_p^{'}$, in sta elementa 1 in $p-1$ edina sama sebi inverzna, ostali elementi $2, 3, \ldots, p-2$ nastopajo v parih (a,b), za katere velja

$$a\,b \equiv 1 \pmod{p}\,.$$

Torej je

$$(p-1)! = 1\cdot 2\cdot 3\cdots(p-1) \equiv 1\cdot 1\cdot 1\cdots 1\cdot(p-1) \equiv p-1 \equiv -1 \pmod{p}\,.$$

Naj bo sedaj p tako naravno število, da je

$$(p-1)! \equiv -1 \pmod{p}\,. \tag{1.11}$$

Denimo, da je p sestavljeno število, torej $p = p_1\,p_2$, kjer je $1 < p_i < p-1$, $i = 1, 2$. Števili p_1 in p_2 torej delita $(p-1)!$, torej tudi p deli $(p-1)!$. To pa je v protislovju z (1.11), torej je p praštevilo. □

Dokaz naslednje karakterizacije praštevilskih dvojčkov najdemo v [1].

IZREK 1.7. *Naj bo $m \in \mathbb{N}$, $m > 2$. Števili m in $m+2$ sta praštevilska dvojčka natanko tedaj, ko je*

$$4((m-1)!+1) + m \equiv 0 \pmod{m(m+2)}\,.$$

Dokaz. Naj bo

$$4((m-1)!+1)+m \equiv 0 \pmod{m(m+2)}. \tag{1.12}$$

Število m torej deli $(m-1)!+1$, zato je po Wilsonovem izreku praštevilo. Iz (1.12) takoj dobimo, da je

$$4(m+1)!+(4+m)m(m+1) \equiv 0 \pmod{m(m+2)},$$

oziroma

$$4((m+1)!+1)+(m+2)(m^2+3\,m-2) \equiv 0 \pmod{m(m+2)},$$

od koder sledi, da $m+2$ deli $4((m+1)!+1)$ in je, ponovno po Wilsonovem izreku, praštevilo.
Privzemimo sedaj, da sta m in $m+2$ praštevili. Spet uporabimo Wilsonov izrek in ugotovimo, da je

$$(m-1)!+1 \equiv 0 \pmod{m}, \tag{1.13}$$
$$(m+1)!+1 \equiv 0 \pmod{m+2}. \tag{1.14}$$

Preprost račun pokaže, da iz (1.14) sledi

$$2(m-1)!+1 \equiv (m-1)(m+2)(m-1)! \equiv 0 \pmod{(m+2)},$$

oziroma

$$2(m-1)!+1 = k\,(m+2), \quad k \in \mathbb{N}. \tag{1.15}$$

Po (1.13) je $(m-1)!+1 = \ell\, m$, od koder sledi

$$2\,k+1 \equiv 0 \pmod{m},$$

oziroma $2\,k+1 = q\,m$, $q \in \mathbb{N}$. Slednjo zvezo vstavimo v (1.15) in dobimo

$$2(m-1)!+1 = \frac{q\,m-1}{2}(m+2),$$

torej

$$4((m-1)!+1)+m \equiv 0 \pmod{m(m+2)},$$

ker je bilo treba pokazati. □

Trenutno največji par praštevilskih dvojčkov sta števili $2003663613 \times 2^{195000} \pm 1$.
Brez dokaza navedimo zelo zanimiv rezultat o praštevilskih dvojčkih.

Izrek 1.8 (Brunov izrek). *Vsota recipročnih vrednosti praštevilskih dvojčkov je končna, torej*

$$\sum_{p,p+2\in\mathbb{P}} \left(\frac{1}{p}+\frac{1}{p+2}\right) = B_2 \approx 1.902160583104 < \infty.$$

Opomba: Oceno za konstanto B_2 so dobili s seštevanjem vseh praštevilskih dvojčkov do približno 10^{16}.

1.11.2 Mersennova praštevila

Mersennova števila smo že spoznali v enem od dokazov o neskončnosti praštevil. Spomnimo se, n-to Mersennovo število je število $M_n = 2^n - 1$. Če je Mersennovo število praštevilo, mu pravimo Mersennovo praštevilo. Primeri Mersennovih praštevil so M_2, M_3, M_5, M_7, M_{13},...

Domneva 1.2. *Mersennovih praštevil je neskončno.*

Znano pa je, da Mersennovo število M_n ne more biti praštevilo, če n ni praštevilo.

Izrek 1.9. *Če je Mersennovo število M_n praštevilo, je tudi n praštevilo.*

Dokaz. Denimo, da je n sestavljeno število, torej $n = p\,q$, $p, q > 1$. Potem je

$$2^n - 1 = 2^{p\,q} - 1 = (2^p - 1)(2^{p(q-1)} + 2^{p(q-2)} + \cdots + 2^p + 1),$$

torej je M_n sestavljeno število. □

Mersennova števila so tesno povezana s perfektnimi števili.

Definicija 1.16. *Naravno število n je perfektno število, če je enako vsoti vseh svojih pravih deliteljev.*

Primeri perfektnih števil so denimo 6, 28, 496 in 8128. Zanimiv je naslednji izrek.

Izrek 1.10. *Sodo število m je perfektno število natanko tedaj, ko je oblike $m = 2^{n-1}M_n$, kjer je M_n Mersennovo praštevilo.*

Dokaz. Naj bo $\sigma : \mathbb{N} \to \mathbb{N}$, kjer je $\sigma(q)$ vsota vseh pozitivnih deliteljev števila q. Zlahka se prepričamo, da je $\sigma(p) = p + 1$ in $\sigma(p^k) = (p^{k+1} - 1)/(p - 1)$, če je p praštevilo. Malo več dela je za dokaz dejstva, da je σ multiplikativna funkcija, zato ga bomo izpustili.
Predpostavimo, da je M_n Mersennovo praštevilo. Potem je

$$\sigma(m) = \sigma\left(2^{n-1}M_n\right) = (2^n - 1)\,(M_n + 1) = M_n\,2^n = 2\,m,$$

torej je m perfektno število.
Privzemimo sedaj, da je m sodo perfektno število in ga zapišimo v obliki $m = 2^{n-1}m_1$, kjer je $n \geq 2$ in m_1 liho število. Potem je

$$\sigma(m) = \sigma\left(2^{n-1}\right)\sigma(m_1) = (2^n - 1)\,\sigma(m_1).$$

Ker je m perfektno število, je $\sigma(m) = 2\,m = 2^n\,m_1$, zato je

$$2^n\,m_1 = (2^n - 1)\,\sigma(m_1).$$

Od tod vidimo, da $2^n - 1$ deli m_1, torej je $m_1 = (2^n - 1)\ m_2$ in zato $\sigma(m_1) = 2^n\,m_2$. Števili m_1 in m_2 obe delita m_1, zato je

$$2^n\,m_2 = \sigma(m_1) \geq m_1 + m_2 = (2^n - 1)\,m_2 + m_2 = 2^k m_2.$$

Torej mora biti $\sigma(m_1) = m_1 + m_2$, kar pomeni, da je m_1 praštevilo in $m_2 = 1$ (saj ima samo dva pozitivna delitelja). Ker je $m_1 = 2^n - 1 = M_n$, je M_n Mersennovo praštevilo in dokaza je konec.

□

1.11.3 Fermatova praštevila

Omenili smo že Fermatova števila

$$F_n = 2^{2^n} + 1, \quad n \in \mathbb{N} \cup \{0\}.$$

Vemo, da so F_n, $n = 0, 1, 2, 3, 4$, praštevila. Slavna domneva o Fermatovih številih je naslednja.

Domneva 1.3. *Fermatovo število F_n, $n \geq 5$ je sestavljeno število.*

Največje trenutno znano sestavljeno Fermatovo število je $F_{2543548}$.
Da pa se dokazati naslednjo lemo, ki je povezana s Fermatovimi števili.

Lema 1.5. *Če je $2^n + 1$ liho praštevilo, je n potenca števila 2.*

Dokaz. Za $n + 1$ lema očitno drži. Denimo, da je $n > 1$ naravno število, ki ni potenca števila 2. Potem je $n = k\,\ell$, $1 \leq k < n$, $1 < \ell \leq n$ in ℓ liho število. Za celi števili a in b in naravno število m je $a^m - b^m$ deljivo z $a - b$. Izberimo $a = 2^k$, $b = -1$ in $m = \ell$. Torej

$$(2^k + 1) | (2^{k\ell} + 1) = 2^n + 1.$$

Ker je $1 < 2^k + 1 < 2^n + 1$, število $2^n + 1$ torej ne more biti praštevilo. □

Poznamo tudi posplošena Fermatova števila.

Definicija 1.17. *Naj bo $a \in \mathbb{N}$, $a > 2$. Številu*

$$G_{n,a} = a^{2^n} + 1, \quad n \in \mathbb{N} \cup \{0\},$$

Rečemo posplošeno Fermatovo število.

V naslednji lemi karakteriziramo prafaktorje posplošenih Fermatovih števil.

LEMA 1.6. *Naj bo p lihi praštevilski faktor posplošenega Fermatovega števila $G_{n,a}$. Potem je $p = k\,2^{n+1} + 1$, $k \in \mathbb{N}$.*

DOKAZ. Naj bo p lihi praštevilski faktor $G_{n,a}$ Potem je

$$a^{2^n} \equiv -1 \pmod{p}. \tag{1.16}$$

Torej je tudi

$$a^{2^{n+1}} \equiv 1 \pmod{p}.$$

Torej je $r = 2^{n+1}$ najmanjše naravno število r, za katerega je

$$a^r \equiv 1 \pmod{p}.$$

Je res najmanjše tako? Pa denimo, da obstaja tako število $1 < r_1 < r$, da je

$$a^{r_1} \equiv 1 \pmod{p}.$$

Potem r_1 deli $r = 2^{n+1}$. Toda $r_1 < r$, zato je $r_1 = 2^e$, $e \leq n$. Od tod sledi, da je

$$a^{2^n} \equiv 1 \pmod{p}.$$

Skupaj z (1.16) pridemo do protislovja $0 \equiv -2 \pmod{p}$.
Vzemimo multiplikativno grupo $\mathbb{Z}_p'$ ostankov po modulu p. Njen red je $p-1$, zato mora r deliti $p-1$. Torej je $p = k\,2^{n+1} + 1$, $k \in \mathbb{N}$. □

OPOMBA. *Za $a = 2$, torej v primeru klasičnih Fermatovih števil, velja še več: p mora biti oblike $k\,2^{n+2} + 1$. Oglejte si denimo primer F_5.*

1.12 Porazdelitev praštevil

V tem razdelku si bom ogledali nekaj elementarnih dejstev o porazdelitvi praštevil med naravnimi števili. Predvsem nas bo zanimalo, kako hitro raste in kakšni sta spodnja in zgornja meja za funkcijo $\pi : \mathbb{R} \to \mathbb{N} \cup \{0\}$, kjer je $\pi(x)$ enako številu praštevil, manjših od x, torej

$$\pi(x) = \#\{p \in \mathbb{P},\ p \leq x\}.$$

Eden od najpomembnejših izrekov o praštevilih se glasi.

IZREK 1.11. *Za funkcijo π velja*

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$$

Dokaz izreka je preobširen in na nakaterih delih precej tehničen, zato ga ne bomo izdelali. Namesto tega bomo dokazali izrek o naraščanju funkcije π. Potrebovali bomo naslednjo definicijo.

DEFINICIJA 1.18. *Naj bosta $f, g : [0, \infty) \to \mathbb{R}$ dve realni funkciji*[1]*. Potem oznaka*

$$f = \Theta(g)$$

pomeni, da obstajata konstanti c in d, da od nekega x naprej velja

$$c\, g(x) \leq f(x) \leq d\, g(x).$$

Podobno oznaka

$$f = \Omega(g)$$

pomeni, da obstaja taka konstanta c, da je od nekega x naprej $f(x) \geq c\, g(x)$.

IZREK 1.12 (Izrek Čebiševa). *Za funkcijo π velja*

$$\pi(x) = \Theta\left(\frac{x}{\log x}\right).$$

Izrek bomo dokazali z nekaj pomožnimi lemami.

LEMA 1.7. *Naj bo $m \in \mathbb{N}$. Potem je*

$$\binom{2m}{m} \geq \frac{2^{2m}}{2m} \qquad \text{in} \qquad \binom{2m+1}{m} < 2^{2m}.$$

DOKAZ. Binomski simbol $\binom{2\,m}{m}$ je največi sumand v razvoju izraza $(1+1)^{2m}$. Zato je

$$2^{2m} = \sum_{i=0}^{2m} \binom{2m}{i} = 1 + \sum_{i=1}^{2m-1} \binom{2m}{i} + 1 \leq 2 + (2m-1)\binom{2m}{m} < 2m\binom{2m}{m}.$$

Pri tem smo upoštevali, da je $2 - \binom{2m}{m} < 0$ za $m > 0$, kar sledi denimo iz lastnosti Pascalovega trikotnika.

[1] V resnici je dovolj, da sta definirani od nekega pozitivnega števila naprej.

Za dokaz druge neenakosti opazimo, da je $\binom{2m+1}{m} = \binom{2m+1}{m+1}$. Torej je

$$\begin{aligned} 2^{2m+1} &= \sum_{i=0}^{2m} \binom{2m}{i} = \sum_{i=0}^{m-1} \binom{2m}{i} + 2\binom{2m+1}{m} + \sum_{i=m+2}^{2m+1} \binom{2m+1}{i} \\ &> 2\binom{2m+1}{m}, \end{aligned}$$

od koder takoj sledi željena neenakost. □

Uvedimo funkcijo $\nu_p : \mathbb{N} \to \mathbb{N} \cup \{0\}$, kjer je $\nu_p(n)$ največji eksponent k, da je n še deljiv s p^k. Natančneje

$$\nu_p(n) = \max\{k \in \mathbb{N} \cup \{0\},\ n \equiv 0 \pmod{p^k}\}.$$

Lema 1.8. *Naj bo $n \in \mathbb{N}$. Za vsako praštevilo p je*

$$\nu_p(n!) = \sum_{k \geq 1} \left\lfloor n/p^k \right\rfloor.$$

Dokaz. Za poljuben par naravnih števil j in k definirajmo $d_{jk} := 1$, če p^k deli j in $d_{jk} := 0$ sicer. Potem je $\nu_p(j) = \sum_{k \geq 1} d_{jk}$ (vsota je končna, saj je $p^k > j$ za dovolj velik k). Torej je

$$\nu_p(n!) = \sum_{j=1}^{n} \nu_p(j) = \sum_{j=1}^{n} \sum_{k \geq 1} d_{jk} = \sum_{k \geq 1} \sum_{j=1}^{n} d_{jk}.$$

Toda $\sum_{j=1}^{n} d_{jk}$ prešteje ravno število večkratnikov števila p^k med 1 in n. Ker je slednje enako $\lfloor n/p^k \rfloor$, je dokaza konec. □

Sledi izrek, v katerem izpeljemo spodnjo mejo za funkcijo π.

Izrek 1.13. *Za vsako naravno število $n \geq 2$ je*

$$\pi(n) \geq \left(\frac{1}{2}\log 2\right) \frac{n}{\log n}.$$

Dokaz. Naj bo m naravno število. Definirajmo

$$N := \binom{2m}{m} = \frac{(2m)!}{(m!)^2}.$$

Hitro se lahko prepričamo, da za funkcijo ν_p velja:

- $\nu_p(a^2) = 2\,\nu_p(a)$,
- $\nu_p(a/b) = \nu_p(a) - \nu_p(b)$, če b deli a.

Po lemi 1.8 je

$$\nu_p(N) = \sum_{k\geq 1} \left(\lfloor 2m/p^k \rfloor - 2\,\lfloor m/p^k \rfloor \right)$$

Vsak sumand v zgornji vsoti je bodisi 0, bodisi 1, za $k > \log(2m)/\log p$ pa identično 0. Torej je $\nu_p(N) \leq \log(2m)/\log p$. Od tod sledi, da je

$$\pi(2m)\log(2m) = \sum_{p\leq 2m} \frac{\log(2m)}{\log p}\log p \geq \sum_{p\leq 2m} \nu_p(N)\log p = \log N,$$

pri čemer sumacija teče po vseh praštevilih do $2m$. Po lemi 1.7 je $N \geq 2^{2m}/(2m) \geq 2^m$. Torej skupaj z zgornjo neenakostjo dobimo

$$\pi(2m)\log(2m) \geq m\log 2,$$

oziroma

$$\pi(2m) \geq \left(\frac{\log 2}{2}\right)\frac{2m}{\log(2m)}.$$

S tem je izrek dokazan za soda števila.
Izberimo sedaj liho število $n \geq 3$, torej $n = 2\,m - 1$, $m \geq 2$. S preprostim računom se prepričamo, da funkcija $f(x) = x/\log x$ narašča za $x \geq 3$. Torej je

$$\pi(2\,m-1) = \pi(2m) \geq \left(\frac{\log 2}{2}\right)\frac{2m}{\log(2m)} \geq \left(\frac{\log 2}{2}\right)\frac{2m-1}{\log(2m-1)},$$

kar dokazuje lemo tudi za liha števila. □

Sedaj je preprosto videti, da je $\pi(x) = \Omega(x/\log x)$. Izberimo $c := 1/2(\log 2)$. Potem je za $x \geq 2$

$$\pi(x) = \pi(\lfloor x \rfloor) \geq c\,\lfloor x \rfloor/\log\lfloor x \rfloor \geq c(x-1)/\log x.$$

Od tod takoj dobimo $\pi(x) = \Omega(x/\log x)$.

Za dokaz zgornje meje najprej uvedimo t.i. theta funkcijo Čebiševa

$$\vartheta(x) = \sum_{p\leq x} \log p,$$

kjer, kot ponavadi, vsota teče po praštevili do x. Od tu naprej bomo povsod po tihem privzeli, da so vse sumacije po spremenljivki p mišljene po praštevilih. Tako denimo lahko pišemo $\pi(x) = \sum_{p\leq x} 1$.

IZREK 1.14. *Za funkcijo ϑ je*

$$\vartheta(x) = \Theta(\pi(x)\log x).$$

DOKAZ. Dokaz je preprost, saj je

$$\vartheta(x) = \sum_{p\le x} \log p \le \log x \sum_{p\le x} 1 = \pi(x)\log x.$$

Po drugi strani je

$$\begin{aligned}\vartheta(x) &= \sum_{p\le x} \log p \ge \sum_{\sqrt{x}<p\le x} \log p \ge \log\sqrt{x} \sum_{\sqrt{x}<p\le x} 1 \\ &= \frac{1}{2}\log x\left(\pi(x) - \pi(\sqrt{x})\right) = \frac{1}{2}\left(1 - \pi(\sqrt{x})/\pi(x)\right)\pi(x)\log x.\end{aligned}$$

Dovolj je torej videti, da je $\lim_{x\to\infty} \pi(\sqrt{x})/\pi(x) = 0$.
Očitno je $\pi(\sqrt{x}) \le \sqrt{x}$. Iz prejšnjega izreka hitro zaključimo, da obstaja taka konstanta c, da je $\pi(x) \ge c\,x/\log x$ za dovolj velike x. Torej za take x sledi

$$\frac{\pi(\sqrt{x})}{\pi(x)} \le \frac{\sqrt{x}}{c\,x/\log x} = \frac{\log x}{c\sqrt{x}} \to 0, \quad x\to\infty.$$

□

IZREK 1.15. *Za $x \ge 1$ je $\vartheta(x) < 2(\log 2)x$.*

DOKAZ. Dovolj je dokazati, da je $\vartheta(n) < 2(\log 2)n$ za $n \in \mathbb{N}$, saj je potem

$$\vartheta(x) = \vartheta(\lfloor x\rfloor) < 2(\log 2)\lfloor x\rfloor \le 2(\log 2)x.$$

Uporabili bomo dokaz z indukcijo. Za $n = 1, 2$ je trditev očitna. Privzemimo torej, da je $n > 2$. Če je n sodo število, iz indukcijske predpostavke sledi

$$\vartheta(n) = \vartheta(n-1) < 2(\log 2)(n-1) < 2(\log 2)n.$$

Naj bo sedaj n liho število, $n = 2\,m + 1$, $m \ge 1$. Definirajmo

$$M := \binom{2\,m+1}{m} = \frac{(2\,m+1)(2\,m)\cdots(m+2)}{m!}.$$

Opazimo, da je število M deljivo z vsemi praštevili p, za katere je $m+1 < p \le 2\,m+1$. Torej je

$$\vartheta(2\,m+1) - \vartheta(m+1) = \sum_{m+1<p\le 2m+1} \log p < \log M.$$

Po lemi 1.7 je $M < 2^{2m}$, zato je

$$\vartheta(2\,m+1) - \vartheta(m+1) < 2(\log 2)m.$$

Iz tega in indukcijske predpostavke za $m+1$ sledi

$$\begin{aligned}\vartheta(n) &= \vartheta(2\,m+1) - \vartheta(m+1) + \vartheta(m+1) < 2(\log 2)m + 2(\log 2)(m+1)\\ &= 2(\log 2)(2\,m+1) = 2(\log 2)n,\end{aligned}$$

kar smo želeli pokazati. □

Povzemimo rezultate zadnjih treh izrekov:

- $\pi(x) \geq c_1\, x/\log x, \quad x \geq 2,$
- $c_2\,\pi(x)\log x \leq \vartheta(x) \leq c_3\,\pi(x)\log x,$
- $\vartheta(x) \leq 2(\log 2)x, \quad x \geq 1.$

Iz tega takoj sledi rezultat izreka 1.12.

Poglavje 2

Polinomi in njihove ničle

2.1 Uvod

Polinomi so ena najpomembnejših matematičnih struktur nasploh. Brez njih računalniki ne bi bili sposobni izračunati praktično ničesar. Kljub temu, da jih ponavadi uvedemo zaradi računskih potreb, jih lahko definiramo tudi zelo formalno, kot algebraično strukturo. V nadaljevanju bomo privzeli, da je množica $A \neq \{0\}$, opremljena z adicijo multiplikacijo, celostno polje, torej komutativen kolobar z enoto brez deliteljev niča. Nekateri rezultati veljajo tudi v primeru, ko je A samo kolobar, a tega ne bomo posebej izpostavljali. Nekateri rezultati pa bodo res samo za polja, torej komutativne obsege, a bomo to posebej poudarili. V primerih bo A ponavadi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ali $\mathbb{C}$.

2.2 Formalna konstrukcija polinomov

V tem razdelku bomo definirali polinome kot zaporedja s končno mnogo od nič različnimi elementi (glejte na primer [4]). Na njih bomo definirali operaciji seštevanja in množenja, kar bo porodilo strukturo kolobarja.
Naj bo $\mathcal{S}$ množica zaporedij s končnim nosilcem, torej

$$\mathcal{S} = \{(a_0, a_1, a_2, \dots);\ a_i \in A,\ i = 0, 1, \dots\},$$

pri čemer je v vsakem zaporedju samo končno mnogo elementov a_i različnih od 0 (z 0 bomo označevali tako nevtralni element za seštevanje v A, kot tudi 0 kot naravno število). Obstaja torej $n \in \mathbb{N}$ (k naravnim številom štejemo tudi 0), da je $a_j = 0$ za vsak $j \geq n$. Množico $\mathcal{S}$ opremimo z operacijama seštevanja $+$ in množenja $\cdot$.

DEFINICIJA 2.1. *Za* $P = (a_0, a_1, \dots)$ *in* $Q = (b_0, b_1, \dots)$ *iz* $\mathcal{S}$ *naj bo*

$$P + Q = (a_0 + b_0, a_1 + b_1, \dots),$$
$$P \cdot Q = (a_0\, b_0, a_0\, b_1 + a_1\, b_0, \dots, a_0\, b_i + a_1\, b_{i-1} + \cdots + a_i\, b_0, \dots).$$

Iz zgornje definicije je očitno, kako seštejemo dva polinoma. Postopek je enak, kot bi seštevali dva vektorja v končnodimenzionalnem prostoru (ne pozabimo, da imajo zaporedja samo končno mnogo neničelnih elementov). Množenje je malce bolj zapleteno. Seveda ga poznamo že iz srednje šole, kjer smo se srečali s klasičnimi polinomi. Kot temu radi rečemo, množimo "vsakega z vsakim". Tu pa si na kratko oglejmo, kako lahko množenje izvedemo malo bolj formalno.
Naj bosta $P, Q \in \mathcal{S}$ in $R = P \cdot Q$. Označimo $R = (c_0, c_1, \dots, c_i, \dots)$. Najprej opazimo, da je $R \in \mathcal{S}$, saj ima končno mnogo neničelnih elementov. Torej je množenje dobro definirano. Oglejmo si definicijo elementa $c_i = a_0\, b_i + a_1\, b_{i-1} + \cdots + a_i\, b_0$. Če definiramo $\boldsymbol{a}_i = (a_0, a_1, \dots, a_i)$ in $\boldsymbol{b}_i = (b_0, b_1, \dots, b_i)$ ter $\mathrm{fliplr}(\boldsymbol{a}_i) = (a_i, a_{i-1}, \dots, a_1, a_0)$, potem je

$$c_i = \mathrm{fliplr}(\boldsymbol{a}_i) .\cdot \boldsymbol{b}_i, \quad i = 0, 1, \dots$$

Pri tem $.\cdot$ pomeni množenje po komponentah[1], torej za vektorja $\boldsymbol{c}_i = (c_0, c_1, \dots, c_i)$ in $\boldsymbol{d}_i = (d_0, d_1, \dots, d_i)$ velja

$$\boldsymbol{c}_i .\cdot \boldsymbol{d}_i = c_0 \cdot d_0 + c_1 \cdot d_1 + \cdots + c_i \cdot d_i.$$

Struktura $(\mathcal{S}, +, \cdot)$ je *kolobar polinomov* nad kolobarjem koeficinetov A (dokaz je preprost, zahtevnejši bralec naj ga izdela sam). Poseben pomen ima element $X = (0, 1, 0, \dots)$, saj je

$$X^k = (\underbrace{0, 0, \dots, 0}_{k-\text{krat}}, 1, 0, \dots), \quad k \in \mathbb{N}.$$

Elementu X rečemo spremenljivka ali nedoločenka nad A. Če nadalje element $a_i \in A$ identificiramo z elementom $(a_i, 0, \dots) \in \mathcal{S}$, lahko polinom $P = (a_0, a_1, \dots)$ zapišemo kot

$$P = a_0 + a_1\, X + a_2\, X^2 + \cdots + a_n\, X^n.$$

Kolobar polinomov $(\mathcal{S}, +, \cdot)$ označimo z $A[X]$.

[1]Množenje po komponentah je denimo zelo značilna operacija v programskem paketu Matlab (kaj več o Matlabu lahko izveste v [9]).

DEFINICIJA 2.2. *Naj bo $P = (a_0, a_1, \dots) \in A[X]$. Če je $a_i = 0$ za vsak $i \in \mathbb{N}$, polinomu P rečemo ničelni polinom in pišemo $P = 0$. Če $P \neq 0$, naj bo $n \in \mathbb{N}$ največje naravno število, za katerega je $a_n \neq 0$. Potem je $n = \deg(P)$ stopnja polinoma P (pri tem definiramo $\deg(0) = -\infty$). Koeficinetu a_n rečemo vodilni koeficient polinoma P, členu $a_n X^n$ pa vodilni člen polinoma P. Če je $a_n = 1$ (kjer je 1 enota kolobarja A), potem polinomu P rečemo monični polinom.*

Za vodilni koeficient in vodilni člen bomo uporabljali oznaki $\mathrm{lc}(P)$ in $\mathrm{lt}(P)$.

PRIMER 2.1. *Naj bo $A = \mathbb{Z}$ in $P = (1, 2, 0, 1, 0, \dots)$ ter $Q = (1, -1, 0, \dots)$. Potem je $P = 1 + 2X + X^3$, $Q = 1 - X$, $P + Q = 2 + X + X^3$ in $P \cdot Q = 1 + X - 2X^2 + X^3 - X^4$. Stopnja polinoma P je $\deg(P) = 3$, njegov vodilni koeficinet $\mathrm{lc}(P) = 1$, vodilni člen polinoma Q pa je $\mathrm{lt}(Q) = -X$.*

Pravkar defninirani polinomi so algebarična struktura. Če želimo s polinomi tudi "računati", potrebujemo naslednjo definicijo.

DEFINICIJA 2.3. *Naj bo $P \in A[X]$. Funkcija $\widetilde{P} : A \to A$ je definirana kot*

$$\widetilde{P}(\alpha) = a_0 + a_1 \alpha + \cdots + a_n \alpha^n$$

in ji rečemo polinomska funkcija polinoma P. Včasih jo označimo kar s P.

OPOMBA. *Premislite, ali imata lahko dva različna polinoma iz $A[X]$ enako polinomsko funkcijo?*

2.3 Evklidov algoritem

V tem sestavku si bomo na kratko ogledali deljivost polinomov iz $A[X]$ in način, kako polinome delimo.

DEFINICIJA 2.4. *Naj bosta $P_1, P_2 \in A[X]$. Pravimo, da polinom P_1 deli polinom P_2, če obstaja polinom Q, da velja $P_2 = P_1 \cdot Q$.*

V nadaljevanju si bomo ogledali način, kako ugotovimo, ali nek polinom deli drugega. Dokažimo najprej naslednji izrek.

IZREK 2.1. *Naj bosta $P_1, P_2 \in A[X]$ polinoma. Če je P_2 monični polinom, potem obstajata taka enolično določena polinoma $Q, R \in A[X]$, da je*

$$P_1 = Q\,P_2 + R, \quad \deg(R) < \deg(P_2)\,.$$

OPOMBA. *Polinom R je lahko 0, saj je po dogovoru* $\deg(0) = -\infty$*, torej je* $\deg(0) < \deg(P_2)$.

DOKAZ. Naj bo $m = \deg(P_1)$ in $n = \deg(P_2)$. Če je $m < n$, vzamemo $Q = 0$ in $R = P_1$.
Naj bo torej $m \geq n$ in $P_1 = a_0 + a_1 X + \cdots + a_m X^m$. Obstoj polinomov Q in R bomo dokazali z indukcijo na m.
Če je $m = n$, je $P_1 = a_m P_2 + (P_1 - a_m P_2)$ in je $Q = a_m$, $R = P_1 - a_m P_2$. Ker je $\deg(R) < \deg(P_1) = \deg(P_2)$, je obstoj iskanih polinomov Q in R v tem primeru dokazan. Denimo, da je res tudi $P_1 = \widetilde{a}_m P_2 + R_1$, kjer je $\deg(R_1) < \deg(P_2)$. Potem je

$$(a_m - \widetilde{a}_m) P_2 = R - R_1.$$

Toda $\deg(R - R_1) < \deg(P_2)$, polinom P_2 pa je moničen, zato mora biti $(a_m - \widetilde{a}_m) \cdot 1 = 0$. Ker je A brez deliteljev niča, je $a_m = \widetilde{a}_m$. Od tod pa takoj sledi tudi $Q = Q_1$. Torej sta Q in R enolično določena.
Naj bo sedaj $m > n$ in naj izrek drži za naravna števila $n, n+1, \ldots, m-1$. Definirajmo

$$F_1 = P_1 - a_m X^{m-n} P_2.$$

Ker je $\deg(F_1) < \deg(P_1) = m$, po indukcijski predpostavki obstajata enolično določena polinoma Q_1 in R_1, $\deg(R_1) < \deg(P_2)$, da je

$$F_1 = Q_1 P_2 + R_1.$$

Če sedaj za vzamemo $Q = a_m X^{m-n} + Q_1$ in $R = R_1$, je

$$P_1 = Q P_2 + R, \quad \deg(R) < \deg(P_2)$$

in izrek je dokazan. □

DEFINICIJA 2.5. *Polinomu R iz prejšnjega izreka rečemo ostanek pri deljenju P_1 s P_2, polinomu Q pa kvocient.*

OPOMBA. *Zahtevo o moničnosti polinoma P_2 lahko izpustimo, če je A polje ali pa v primeru, ko je vodilni koeficient polinoma P_2 obrnljiv element kolobarja A.*

Deljenje polinoma P_1 s polinomom P_2 je mogoče izvesti algoritmično, torej v končnem številu korakov priti do polinomov Q in R. Postopek je znan kot Evklidov algoritem.

function EVKLID(P_1,P_2)
//Podatki: P_1 in P_2 polinoma, P_2 moničen.
//Rezultat: kvocient Q in ostanek R.
$R \leftarrow P_1$
$Q \leftarrow 0$;
while $\deg(R) \geq \deg(P_2)$ **do**
$G \leftarrow \mathrm{lc}(R)\, X^{\deg(R)-\deg(P_2)}$
$Q \leftarrow Q + G$
$R \leftarrow R - G\, P_2$
end while
end function

Algoritem 2.1: Evklidov algoritem.

PRIMER 2.2. *Naj bo* $P_1 = 1 + X - X^3 + 2\,X^4$ *in* $P_2 = 2 - X + X^2$. *Z Evklidovim algoritmom določite kvocient in ostanek pri deljenju polinoma* P_1 *s* P_2.
Uporabimo algoritem 2.1 in dobimo $Q = -3 + X + 2\,X^2$ *in* $R = 7 - 4\,X$.

Oglejmo si pomembno uporabo Evklidovega algoritma.

DEFINICIJA 2.6. *Naj bosta* $P_1, P_2 \in A[X]$ *polinoma. Polinom* $G \in A[X]$ *je največji skupni delitelj polinomov* P_1 *in* P_2, *če* G *deli* P_1 *in* P_2 *ter za vsak drug delitelj* H *polinomov* P_1 *in* P_2 *velja, da* H *deli* G. *Polinom* G *(če obstaja), bomo označevali z* $\gcd(P_1, P_2)$.

Celostni domeni A, v kateri poljubna dva elementa premoreta največji skupni delitelj, pravimo GCD-domena. Primer take domene je denimo kolobar celih števil. Posebej je vsako polje k (komutativen obseg) GCD-domena. V tem primeru lahko največji skupni delitelj dveh polinomov $P_1, P_2 \in k[X]$ poiščemo z algoritmom 2.2.

PRIMER 2.3. *Z algoritmom 2.2 poiščite največji skupni delitelj polinomov* $P_1, P_2 \in \mathbb{Q}[X]$, *kjer je*

$$P_1(X) = 1 + 2\,X + 2\,X^2 + X^3 - X^4 - X^5 + X^7 + X^8,$$
$$P_2(X) = 2 + X + X^2 + X^4 + X^5.$$

Dobimo zaporedje $P_1 = Q_1\,P_2 + P_3$, $P_2 = Q_2\,P_3 + P_4$ *in* $P_3 = Q_3\,P_4 + P_5$, *kjer je*

$$P_3(X) = 5 + 4\,X + 4\,X^2 - X^3,$$
$$P_4(X) = -112(1 + X + X^2),$$
$$P_5(X) = 0.$$

```
function GCD(P1,P2)
//Podatki: P1 in P2 polinoma nad poljem k.
//Rezultat: G ← gcd(P1, P2).
    if P2 = 0 then
        G ← P1
    else
        while P2 ≠ 0 do
            P1 = Q P2 + R //Q in R iz Evklidovega algoritma.
            P1 ← P2
            P2 ← R
        end while
        G ← P1
    end if
end function
```

Algoritem 2.2: Največji skupni delitelj (GCD).

Torej je $\gcd(P_1, P_2) = -112(1 + X + X^2)$.

2.4 Ničle polinomov

V tem razdelku si bomo ogledali nekaj splošnih lastnosti, povezanih z ničlami polinomov. Dogovorimo se najprej, kaj izraz ničla sploh pomeni.

Definicija 2.7. *Elementu* $a \in A$ *rečemo ničla polinoma* $P \in A[X]$*, če je* $P(a) = 0$.

Deljivost in ničlo polinoma povezuje naslednja trditev.

Trditev 2.1. *Naj bo* $P \in A[X]$ *in* $a \in A$*. Potem je* a *ničla polinoma* P *natanko tedaj, ko polinom* $X - a$ *deli* $P(X)$*.*

Dokaz. Po Evklidovem algoritmu obstajata enolično določena polinom $Q \in A[X]$ in element $r \in A$, da je $P(X) = (X - a)\,Q(X) + r$. Če je a ničla P, je $P(a) = r = 0$, torej $(X - a)$ deli $P(X)$. Obratno, če $(X - a)$ deli $P(X)$, je po definiciji $P(X) = Q(X)(X - a)$. Toda potem je $P(a) = 0$ in trditev je dokazana. □

Posledica 2.1. *Če so* $a_1, a_2, \ldots, a_m \in A$ *različne ničle polinoma* $P \in A[X]\backslash 0$*, potem polinom* $(X - a_1)(X - a_2) \cdots (X - a_m)$ *deli* $P(X)$ *v* $A[X]$*. Število ničel polinoma* P *v* A *je največ* $\deg(P)$.

Dokaz. Dokazovali bomo z indukcijo na m. Za $m = 1$ rezultat sledi iz trditve 2.1. Predpostavimo torej, da izjava iz posledice drži za nek $m \geq 1$. Potem lahko polinom $P(X)$ zapišemo kot

$$P(X) = (X - a_1)(X - a_2) \cdots (X - a_{m-1})Q(X), \quad Q \in A[X]. \tag{2.1}$$

Torej je $P(a_m) = (a_m - a_1)(a_m - a_2) \cdots (a_m - a_{m-1})Q(a_m) = 0$. Ker je A brez deliteljev niča in je $a_m \neq a_i$, $i = 1, 2, \ldots, m-1$, mora biti $Q(a_m) = 0$. Tedaj pa lahko (ponovno po trditvi 2.1) polinom $Q(X)$ zapišemo kot $Q(X) = (X - a_m)R(X)$, $R \in A[X]$ in iz (2.1) sledi, da $(X - a_1)(X - a_2) \cdots (X - a_m)$ deli $P(X)$ v $A[X]$.
Iz zveze

$$P(X) = (X - a_1)(X - a_2) \cdots (X - a_m)R(X)$$

sledi tudi $m \leq \deg\left((X - a_1)(X - a_2) \cdots (X - a_m)R(X)\right) = \deg(P)$, kar je bilo treba dokazati. □

Opomba. *Če ima A delitelje niča, potem obstaja polinom $P \in A[X]$, ki ima več kot* $\deg(P)$ *različnih ničel. Oglejte si denimo polinom $P(X) = a\,X$, kjer je a kak delitelj niča.*

Za polinom $P(X) = 1 - 2\,X + X^2$ iz $\mathbb{Z}[X]$ opazimo, da se da zapisati kot $P(X) = (1 - X)(1 - X) = (1 - X)^2$. Torej ima ničlo $a_1 = 1$, ki se pojavi dvakrat. Taki ničli rečemo večkratna in jo formalno definiramo takole.

Definicija 2.8. *Naj bo $P \in A[X]$ in $a \in A$. Element a je ničla stopnje $k \geq 1$ polinoma $P(X)$, če $(X - a)^k$ deli $P(X)$ v $A[X]$, $(X - a)^{k+1}$ pa ne deli $P(X)$ v $A[X]$. Število k se imenuje večkratnost ničle a.*

Trditev 2.2. *Naj bo $P \in A[X]$ in $a \in A$. Potem je a ničla stopnje $k \geq 1$ natanko tedaj, ko obstaja tak polinom $Q \in A[X]$, da je*

$$P(X) = (X - a)^k Q(X), \quad Q(a) \neq 0.$$

Dokaz. Naj bo a ničla stopnje k. Po definiciji je $P(X) = (X - a)^k Q(X)$. Če bi bilo $Q(a) = 0$, bi po trditvi 2.1 lahko pisali $P(X) = (X - a)^{k+1} Q_1(X)$, kar je v protislovju z definicijo večkratnosti.
Privzemimo sedaj, da je $P(X) = (X - a)^k Q(X)$ in $Q(a) \neq 0$. Denimo, da je tudi $P(X) = (X - a)^{k+1} Q_1(X)$. Potem je $(X - a)^k (Q(X) - (X - a)Q_1(X)) \equiv 0$. Toda $A \neq \{0\}$ je celostno območje, torej je tak tudi kolobar $A[X]$ (poskusite dokazati), zato mora biti $Q(X) = (X - a)Q_1(X)$ in posledično $Q(a) = 0$, kar je protislovje. □

TRDITEV 2.3. *Če je $P \in A[X]\backslash\{0\}$, potem je vsota večkratnosti ničel polinoma P, ki so v A, največ* $\deg(P)$.

DOKAZ. Naj bodo a_i, $i = 1, 2, \ldots, m$, različne ničle polinoma P v A z večkratnostmi s_i, $i = 1, 2, \ldots, m$. Po prejšnji trditvi obstaja tak polinom $Q \in A[X]$, da je

$$P(X) = \prod_{i=1}^{m} (X - a_i)^{s_i} Q(X).$$

Od tod sledi, da je

$$\deg(P) = \deg\left(\prod_{i=1}^{m} (\cdot - a_i)^{s_i} Q\right) \geq \deg\left(\prod_{i=1}^{m} (\cdot - a_i)^{s_i}\right) = \sum_{i=1}^{m} s_i.$$

□

POSLEDICA 2.2. *Naj bo $P \in A[X]$ in $a_i \in A$, $i = 1, 2, \ldots s$, da je $P(a_i) = 0$, $i = 1, 2, \ldots, s$. Če je $s > \deg(P)$, potem je $P = 0$.*

Zadnje trditve omejujejo število ničel polinoma P in karakterizirajo njihovo večkratnost. Ničesar pa ne povedo o eksistenci ničel. V naslednjem poglavju si bomo ogledali poseben primer polinomov, kompleksne polinome, za katere o eksistenci ničel lahko povemo bistveno več.

Poglavje 3

Kompleksni polinomi

V tem poglavju se bomo omejili na poseben primer polinomov, na kompleksne polinome. To so polinomi nad kolobarjem kompleksnih števil, torej $\mathbb{C}[X]$. Pogosto oznako $\mathbb{C}[X]$ zamenjamo z $\mathbb{C}[z]$, kjer z namiguje na spremenljivko, ki jo v polinomski funkciji zamenjamo s kompleksnim številom $z \in \mathbb{C}$. To oznako od sedaj naprej sprejmimo tudi mi.
Izkazalo se bo, da za kompleksne polinome v splošnem lahko povemo nekaj več kot za polinome nad poljubnim celostnim območjem ali poljem.

3.1 Osnovni izrek algebre

Najprej se posvetimo enemu najpomembnejših izrekov algebre, osnovnemu izreku algebre. Že samo ime nakazuje na njegovo pomembnost. Z znanjem, ki smo si ga pridobili v prejšnjem poglavju, osnovni izrek algebre zlahka formuliramo.

Izrek 3.1 (Osnovni izrek algebre). *Vsak nekonstanten polinom $P \in \mathbb{C}[z]$ ima vsaj eno (kompleksno) ničlo.*

Izrek bomo dokazali postopoma, večinoma sledili [6]. Še prej pa podajmo nekaj komentarjev.
Očitno je, zakaj moramo izločiti konstantne polinome. Če je $P(z) = c \in \mathbb{C}\backslash\{0\}$, potem seveda P ne more imeti ničle. Ničelni polinom $P = 0$ pa ima za ničle kar vsa kompleksna števila, kar je druga skrajnost. Prav tako hitro uvidimo, da izrek ne velja za polinome nad poljem realnih števil $\mathbb{R}[x]$. Preprost protiprimer je denimo polinom $P(x) = 1+x^2$, katerega edini ničli sta $\pm i$, ki pa nista v $\mathbb{R}$. Če za vsak nekonstanen polinom $P \in \mathbb{F}[X]$ velja, da ima vse ničle v $\mathbb{F}$, pravimo, da je polje $\mathbb{F}$ algebraično zaprto. Iz osnovnega izreka algebre v resnici sledi, da je polje kompleksnih števil algebraično zaprto.

Preprosto pa je tudi videti, da nobeno končno polje ne more biti algebraično zaprto.

PRIMER 3.1. *Naj bo $\mathbb{F}$ končno polje, katerega elementi so $\{a_0, a_1, \ldots, a_k\}$. Polinom $P(X) = (X - a_0)(X - a_1)\cdots(X - a_k) + 1$ očitno nima ničle v $\mathbb{F}$, torej polje $\mathbb{F}$ ni algebraično zaprto.*

Na poto do dokaza osnovnega izreka algebre bomo najprej dokazali naslednjo pomembno lemo.

LEMA 3.1. *Naj bo $k \in \mathbb{N}$, $k \geq 2$, in $\xi = \left(1 + \frac{i}{k}\right)^2$. Potem je*

$$\operatorname{Re}\left(\xi^k\right) < 0 < \operatorname{Im}\left(\xi^k\right).$$

DOKAZ. Lemo bomo dokazali analitično, le z uporabo polarnega zapisa in prijemi elementarne enalize. Zapišimo ξ v polarni obliki, torej

$$\xi = \left(1 + \frac{1}{k^2}\right)\left(\cos(2\,\varphi_k) + i\,\sin(2\,\varphi_k)\right), \quad \varphi_k = \arctan\left(\frac{1}{k}\right).$$

Torej je

$$\xi^k = \left(1 + \frac{1}{k^2}\right)^k \left(\cos(2\,k\,\varphi_k) + i\,\sin(2\,k\,\varphi_k)\right).$$

Dovolj je pokazati, da je $2\,k\,\varphi_k \in J := \left(\frac{\pi}{2}, \pi\right)$.
V ta namen si oglejmo funkcijo

$$f(x) = 2\,x\,\arctan\left(\frac{1}{x}\right), \quad x \in I := \left[\sqrt{3}, \infty\right).$$

Lema bo dokazana, če pokažemo, da je $f(I) \subseteq J$.
Ker je

$$f(\sqrt{3}) = 2\,\sqrt{3}\arctan\left(1/\sqrt{3}\right) = \frac{\sqrt{3}}{3}\pi > \sqrt{3},$$

je $f(\sqrt{3}) \in J$. Zaradi

$$\lim_{x\to\infty} f(x) = \lim_{x\to\infty} 2\frac{\arctan\left(\frac{1}{x}\right)}{\frac{1}{x}} = \lim_{x\to 0} 2\,\frac{\arctan x}{x} = \lim_{x\to 0} 2\,\frac{\frac{1}{1+x^2}}{1} = 2 \in J$$

zadošča preveriti, da je f naraščajoča na I. S preprostim računom pridemo do

$$f'(x) = 2\left(\arctan\left(\frac{1}{x}\right) - \frac{x}{1+x^2}\right).$$

Torej je sedaj dovolj videti, da je $f' > 0$ na I. To pa sledi iz zvez

$$f''(x) = -\frac{4}{(1+x^2)^2}, \quad f'(\sqrt{3}) = \frac{2\,\pi}{6} - \frac{2\,\sqrt{3}}{4} > 0, \quad \lim_{x\to\infty} f'(x) = 0.$$

□

Dokažimo sedaj omenjeni izrek.

Dokaz. Naj bo nekonstanten polinom P oblike $P(z) = a_0 + a_1\,z + \cdots + a_n\,z^n$, kjer so koeficienti $a_j \in \mathbb{C}$, $j = 0, 1, \ldots n$, $a_n \neq 0$, $n \geq 1$. Potem je za vsako kompleksno število $z \in \mathbb{C}$,

$$|P(z)| \geq |a_n|\;|z|^n - |a_{n-1}|\;|z|^{n-1} - \cdots - |a_0|\,.$$

Torej je

$$\lim_{|z|\to\infty} |P(z)| = \infty,$$

od koder sedi, da obstaja tak $R > 0$, da je za vsak $z \in \mathbb{C}$, $|z| > R$, $|P(z)| > |P(w)|$, za vsak $w \in \mathbb{C}$, $|w| \leq R$. Množica $\mathcal{K} := \{w \in \mathbb{C};\ |w| \leq R\}$ je kompaktna, P pa zvezna funkcija, zato $|P|$ zavzame globalni minimum na $\mathcal{K}$. Brez škode za splošnost lahko predpostavimo, da je minimum zavzet pri $z_0 = 0$ (saj sicer na začetku premaknemo koordinatni sistem, da je temu tako). Torej je

$$|P(z)|^2 - |P(0)|^2 \geq 0, \quad \text{za vsak } z \in \mathbb{C}, \tag{3.1}$$

in

$$P(z) = P(0) + z^k\,Q(z), \tag{3.2}$$

za nek $k \in \{1, 2, \ldots, n\}$, kjer je Q polinom, za katerega je $Q(0) \neq 0$. Izberimo poljubno realno število $r \geq 0$ ter poljubno kompleksno število $\zeta \in \mathbb{C}$ in si oglejmo (3.1) pri $z = r\,\zeta$. Po (3.2) je

$$\begin{aligned} |P(z)|^2 &= \overline{\left(P(0) + z^k\,Q(z)\right)}\left(P(0) + z^k\,Q(z)\right) \\ &= |P(0)|^2 + 2\,\mathrm{Re}\left(\left(\overline{P(0)}\,z^k\,Q(z)\right)\right) + \left|z^k\,Q(z)\right|^2, \end{aligned}$$

zato

$$|P(r\,\zeta)|^2 - |P(0)|^2 = 2\,r^k \mathrm{Re}\left(\overline{P(0)}\,\zeta^k\,Q(r\,\zeta)\right) + r^{2\,k}\left|\zeta^k\,Q(r\,\zeta)\right|^2 \geq 0, \quad r \geq 0,$$

oziroma

$$2\,\mathrm{Re}\left(\overline{P(0)}\,\zeta^k\,Q(r\,\zeta)\right) + r^k\left|\zeta^k\,Q(r\,\zeta)\right|^2 \geq 0, \quad r > 0,\ \zeta \in \mathbb{C}.$$

Leva stran zadnje neenačbe je zvezna funkcija r na $[0,\infty)$, zato je po limitiranju $r \to 0$

$$\mathrm{Re}\left(\overline{P(0)}\,Q(0)\zeta^k\right) \geq 0, \quad \text{za vsak } \zeta \in \mathbb{C}. \tag{3.3}$$

Naj bo $\alpha := \overline{P(0)}\,Q(0) = a + i\,b$, $a, b \in \mathbb{R}$. Če je k liho število, potem v (3.3) izberemo za $\zeta = \pm 1$ ter $\zeta = \pm i$ in sklepamo, da je $a = b = 0$. Torej je $\alpha = 0$ in zato $P(0) = 0$, kar pomeni, da ima P vsaj eno ničlo.
Naj bo k sodo število. Če v (3.3) izberemo $\zeta = 1$, sledi $a \geq 0$. Izberimo sedaj ζ tako kot v lemi 3.1 in pišimo $\zeta^k = x + i\,y$. Po pravkar omenjeni lemi je $x < 0$ in $y > 0$. Ker (3.3) velja za ζ in $\overline{\zeta}$, je $\mathrm{Re}\,(\alpha(x \pm i\,y)) = a\,x \mp b\,y \geq 0$. Torej je $a\,x \geq 0$ in zato (ker je $x < 0$) $a \leq 0$. Torej je $a = 0$ in $\mp b\,y \geq 0$. Od tod zaradi $y > 0$ sledi $b = 0$, torej tudi $\alpha = 0$ in $P(0) = 0$. Polinom P ima tudi v tem primeru vsaj eno ničlo. □

Posledica 3.1. *Vsak kompleksni polinom $P \in \mathbb{C}[z]$ stopnje $n \geq 1$ ima natanko n kompleksnih ničel (šteto z večkratnostjo).*

Dokaz. Posledico bomo dokazali z indukcijo na stopnjo n.
Naj bo najprej $n = 1$. Ker polinom stopnje $n = 1$ ne more biti konstanten, ima po prejšnjem izreku vsaj eno ničlo $z_1 \in \mathbb{C}$. Potem je $P(z) = (z - z_1)\,Q(z)$, kjer je Q neničelni konstantni polinom.
Privzemimo sedaj, da ima vsak polinom Q stopnje $n \geq 1$, natanko n kompleksnih ničel. Vzemimo poljuben polinom P stopnje $n+1$. Ponovno ima P po že prej omenjenem izreku vsaj eno kompleksno ničlo z_{n+1}. Zato je

$$P(z) = (z - z_{n+1})\,Q(z), \quad \deg(Q) = n.$$

(Če bi bilo $\deg(Q) < n$, potem P ne bi bil stopnje $n+1$.) Po indukcijski predpostavki ima Q natanko n kompleksnih ničel, ki so seveda tudi ničle polinoma P. Torej ima P natanko $n+1$ kompleksnih ničel, kar smo želeli dokazati. □

Pravkar dokazani izrek očitno ni konstruktiven. Zagotovljen je obstoj n ničel kompleksnega polinoma stopnje n, ni pa jasno, kako jih dobimo. V splošnem lahko ničle kompleksnega polinoma poiščemo le numerično, pa še to ponavadi za polinome, katerih koeficienti so realna števila. Le za polinome stopnje ≤ 4 so znane formule v zaključeni obliki, ki podajajo ničle polinoma kot (eksplicitno) funkcijo koeficientov. Za linearni polinom je to očitno, formule za kvadratni polinom se naučimo v srednji šoli, obstajajo pa še Cardanove formule za kubične polinome in formule za ničle polinoma stopnje 4. Za polinome stopnje ≥ 5 je Niels H. Abel dokazal, da v splošnem ni

mogoče izraziti njihovih ničel z eksplicitnimi algebraičnimi operacijami koeficientov. Obstaja pa nekaj ocen o lokaciji ničel kompleksnega polinoma. Najprej si oglejmo peščico rezultatov, ki locirajo ničle polinoma z realnimi koeficienti (realnega polinoma).

3.2 Descartesovo pravilo predznakov

V tem razdelku si bomo ogledali enega od pomembnejših izrekov o številu pozitivnih realnih ničel realnega polinoma. Izrek je znan pod imenom "Descartesovo pravilo predznakov". Še prej si oglejmo nekaj splošnih rezultatov o število pozitivnih in negativnih ničel realnega polinoma. Kot smo navajeni, pišimo nedoločenko kot x, polinom $p \in \mathbb{R}[x]$ pa kot

$$p(x) = a_n\, x^n + a_{n-1}\, x^{n-1} + \cdots + a_1\, x + a_0.$$

Iz koeficientov polinoma p, lahko tvorimo zaporedje $n+1$ realnih števil, ki ga označimo kot vektor

$$\boldsymbol{a} = (a_0, a_1, \ldots, a_n). \tag{3.4}$$

V nadaljevanju bomo potrebovali naslednjo definicijo.

Definicija 3.1. *Pravimo, da sta neničelna člena a_i in a_j zaporedja* (3.4) *zaporedna, če je $j = i+1$, ali pa je $j > i+1$ in je $a_k = 0$ za $k = i+1, i+2, \ldots, j-1$. Sprememba predznaka v zaporedju je par zaporednih členov zaporedja z različnim predznakom. Število sprememb predznaka označimo z $V(\boldsymbol{a}) := V(a_0, a_1, \ldots, a_n)$.*

Primer 3.2. *V zaporedju -2, 3, 4, -1, -2, 2, 3 so tri spremembe predznaka, zato je $V(-2,3,4,-1,-2,2,3) = 3$. V zaporedju 3, 0, 0, -1, 1, 3, 0 pa sta dve spremembi predznaka (par 3, -1 in par -1, 1), zato je $V(3,0,0,-1,1,3,0) = 2$.*

Najprej dokažimo nekaj preprostejših rezultatov.

Lema 3.2. *Če so vsi koeficienti polinoma p pozitivni, potem p nima pozitivnih realnih ničel.*

Dokaz. Če so vsi koeficienti a_i, $i = 0, 1, \ldots, n$, pozitivni, je za vsak $x > 0$ vrednost $p(x)$ očitno pozitivna, torej p nima ničel na $(0, \infty)$. □

Posledica 3.2. *Če je za polinom p število sprememb predznaka $V(\boldsymbol{a}) = n$, potem p nima negativnih ničel.*

Dokaz zadnje posledice prepuščamo bralcu, oglejmo pa si primer uporabe zadnjih dveh trditev.

PRIMER 3.3. *Polinom* $p(x) = x^4 + 10\,x^3 + 35\,x^2 + 50\,x + 24$ *po lemi 3.2 nima pozitivnih ničel. Bralec se res lahko prepriča, da ima ničle pri* $x = -1, -2, -3, -4$.
Po posledici 3.2 pa polinom $p(x) = x^4 - 10\,x^3 + 35\,x^2 - 50\,x + 24$ *nima negativnih ničel. Njegove ničle so* $x = 1, 2, 3, 4$.

TRDITEV 3.1. *Če so vse ničle polinoma p stopnje* $n \geq 1$ *pozitivne, potem je* $V(\boldsymbol{a}) = n$.

DOKAZ. Dokazujmo z indukcijo na n. Za $n = 1$ dejstvo, da ima $p(x) = a_1\,x + a_0$ pozitivno ničlo pomeni, da je $a_1\,a_0 < 0$, torej je $V(\boldsymbol{a}) = 1$. Naj bo sedaj $p(x) = a_{n+1}\,x^{n+1} + a_n\,x^n + \cdots + a_1\,x + a_0$ polinom stopnje $n+1$ s samimi pozitivnimi ničlami ξ_i, $i = 1, 2, \ldots, n+1$. Potem je

$$p(x) = a_{n+1}(x - \xi_1)(x - \xi_2)\cdots(x - \xi_{n+1}).$$

Torej je

$$p(x) = (x - \xi_{n+1})q(x), \tag{3.5}$$

kjer je

$$q(x) = a_{n+1}\,(x - \xi_1)(x - \xi_2)\cdots(x - \xi_n) = b_n\,x^n + b_{n-1}\,x^{n-1} + \cdots + b_1\,x + b_0. \tag{3.6}$$

Polinom q ima same pozitivne ničle, zato je po indukcijski predpostavki $V(\boldsymbol{b}) = n$. Iz zvez (3.5) in (3.6) sledi

$$\begin{aligned} a_0 &= -\xi_{n+1}\,b_0, \\ a_i &= b_{i-1} - \xi_{n+1}\,b_i, \quad i = 1, 2, \ldots, n, \\ a_{n+1} &= b_n, \end{aligned}$$

od tod pa zlahka preverimo, da je $V(\boldsymbol{a}) = n+1$ (saj opazimo, da je predznak b_n enak predznaku a_{n+1}, predznak b_{n-1} enak predznaku a_n,..., predznak b_0 enak predznaku a_1 in zato predznak a_0 nasproten predznaku a_1). □

POSLEDICA 3.3. *Če so vse ničle polinoma p stopnje n negativne, potem je* $V(\boldsymbol{a}) = 0$.

Tudi dokaz te posledice prepuščamo bralcu.

Obrat pravkar zapisane trditve (in posledice) ne velja.

PRIMER 3.4. *Polinom* $p(x) = (x - 1/3)(x - 1/2)(x - 2)(x - 3)$ *ima same pozitivne ničle. Ko ga razpišemo po potencah, dobimo*

$$p(x) = x^4 - \frac{35}{6}x^3 + \frac{31}{3}x^2 - \frac{35}{6}x + 1,$$

torej ima vse koeficinete neničelne z alternirajočimi predznaki.
Po drugi strani pa polinom $p(x) = x^2 + x + 1$ *nima nobene realne ničle (kaj šele vse negativne), pa čeprav so vsi koeficienti neničelni in istega predznaka. To dokazuje, da obrat posledice 3.3 ni mogoč. Podobno dobimo protiprimer tudi za trditev 3.1.*

Sedaj bomo dokazali prvi korak k omenjenemu Descartesovemu izreku. Pokazali bomo, da natanko ena sprememba predznaka v koeficientih polinoma p implicira obstoj natanko ene pozitivne ničle polinoma. Še prej dokažimo naslednji izrek.

IZREK 3.2. *Če je v polinomu* p *stopnje* n *s pozitivnim vodilnim koeficientom pred prvim negativnim koeficientom (gledano od vodilnega koeficienta proti prostemu členu) natanko* k *pozitivnih ali ničelnih koeficientov in* N *označuje absolutno vrednost največjega negativnega koeficienta, potem je* $p(x) > 0$ *za* $x \geq 1 + \sqrt[k]{N/a_n}$. *Polinom* p *ima tedaj torej vse realne ničle na intervalu* $(-\infty, 1 + \sqrt[k]{N/a_n})$.

DOKAZ. Naj za koeficiente a_i, $i = 0, 1, \ldots, n$, v polinomu $p(x) = a_n\, x^n + a_{n-1}\, x^{n-1} + \cdots + a_{n-k+1}\, x^{n-k+1} + a_{n-k}\, x^{n-k} + \cdots + a_1\, x + a_0$ velja $a_n > 0$, $a_i \geq 0$, $i = n - k + 1, n - k + 2, \ldots, n - 1$ in $a_{n-k} < 0$. Potem je za $x > 1$

$$p(x) \geq a_n\, x^n + \sum_{j=0}^{n-k} a_j\, x^j \geq a_n\, x^n - \sum_{j=0}^{n-k} N\, x^j,$$

kjer je

$$N = \max\left\{|a_j|;\ \operatorname{sign}(a_j) = -1,\ 0 \leq j \leq n - k\right\}.$$

Od tod dobimo

$$p(x) > a_n\, x^{k-1}\left(x^{n-k+1} - 1\right) - N\frac{x^{n-k+1} - 1}{x - 1} > \frac{x^{n-k+1} - 1}{x - 1}\left(a_n(x-1)^k - N\right).$$

Ker je $x > 1$, je prvi faktor na desni strani zadnje neenakosti pozitiven. Če je $x \geq 1 + \sqrt[k]{N/a_n}$, je nenegativen še drugi faktor in izrek je dokazan. □

TRDITEV 3.2. *Če za polinom* p *velja* $V(\boldsymbol{a}) = 1$, *potem ima* p *vsaj eno pozitivno ničlo.*

DOKAZ. Brez škode za splošnost lahko predpostavimo, da je $a_0 \neq 0$ (sicer izločimo (večkratno) ničlo $x = 0$). Tedaj iz predpostavke trditve sledi, da je $a_n\, a_0 < 0$. Torej je bodisi $p(0) < 0$ in $p(x) > 0$ za dovolj velike x, bodisi $p(0) > 0$ in $p(x) < 0$ za dovolj velike x. Zaradi zveznosti funkcije p ima slednja vsaj eno ničlo na $(0, \infty)$. □

Za dokaz obstoja natanko ene pozitivne ničle bomo uporabili nekaj lastnosti funkcije $\phi_k(x) = \sum_{j=0}^{k-1} x^j$, $k = 1, 2, \ldots$ Te so:

$$\phi_k(1) = k, \tag{3.7}$$
$$\phi_k(y) \geq \phi_k(x), \quad y \geq x \geq 1, \tag{3.8}$$
$$\phi_\ell(x) \geq \phi_k(x), \quad \ell \geq k, \quad x \geq 0. \tag{3.9}$$

TRDITEV 3.3. *Če za polinom p velja $V(\boldsymbol{a}) = 1$, potem ima p* **natanko eno** *pozitivno ničlo.*

DOKAZ. Brez škode za splošnost lahko privzememo, da je vodilni koeficient polinoma p pozitiven in prosti člen različen od 0 (sicer polinom pomnožimo z -1 in izločimo morebitno večkratno ničlo pri 0, kar ne spremeni vrednosti $V(\boldsymbol{a})$). Po prejšnji trditvi obstaja vsaj ena pozitivna ničla polinoma p. Dokazati moramo, da je edina. Privzemimo, da je pozitivnih ničel več in z α označimo najmanjšo med njimi. Definirajmo polinom $\hat{p}(x) = \alpha^{-n}\, p(\alpha\, x)$. Koeficienti polinoma $\hat{p}$ imajo enake predznake kot koeficienti polinoma p. Najmanjša ničla polinoma $\hat{p}$ pa je $x = 1$. Pokazali bomo, da je $x = 1$ enostavna ničla polinoma $\hat{p}$ in je $\hat{p}(x) > 0$ za $x > 1$.
Ker je $a_n > 0$ po privzetku, lahko $\hat{p}$ zapišemo kot

$$\hat{p}(x) = \sum_{j=n-k+1}^{n} b_j\, x^j - \sum_{j=0}^{n-k} |b_j|\; x^j, \quad 1 \leq k \leq n,$$

kjer je $b_j \geq 0$, $j = n-k+1, \ldots, n$ in $b_j \leq 0$, $j = 0, 1, \ldots, n-k$. Potem je

$$\begin{aligned}\hat{p}(x) = \hat{p}(x) - \hat{p}(1) &= \sum_{j=n-k+1}^{n} b_j (x^j - 1) - \sum_{j=0}^{n-k} |b_j|\, (x^j - 1) \\ &= (x-1) \left(\sum_{j=n-k+1}^{n} b_j\, \phi_j(x) - \sum_{j=1}^{n-k} |b_j|\, \phi_j(x) \right) = (x-1)\, s(x),\end{aligned}$$

kjer je

$$s(x) := \left(\sum_{j=n-k+1}^{n} b_j\, \phi_j(x) - \sum_{j=1}^{n-k} |b_j|\, \phi_j(x) \right).$$

Dovolj je videti, da je s pozitivna funkcija na $[1,\infty)$. Naj bo torej $x \geq 1$. S pomočjo lastnosti (3.7)–(3.9) ocenimo

$$\begin{aligned} s(x) &\geq \phi_{n-k+1}(x) \left(\sum_{j=n-k+1}^{n} b_j - \sum_{j=1}^{n-k} |b_j| \right) \\ &= \phi_{n-k+1}(x) \left(\sum_{j=n-k+1}^{n} b_j - \sum_{j=0}^{n-k} |b_j| + |b_0| \right) \geq \phi_{n-k+1}(1) \left(\hat{p}(1) + b_0 | \right) \\ &= (n-k+1)|b_0| > 0 \end{aligned}$$

in izrek je dokazan. □

Še nekaj splošnih rezultatov o pozitivnih ničlah realnega polinoma bralec lahko najde v [3]. Mi pa se bomo v nadaljevanju posvetili primeru, ko koeficienti realnega polinoma več kot enkrat spremenijo predzak. V tem primeru ne moremo dokazati, da je pozitivnih ničel ravno toliko kot sprememb predznaka.

PRIMER 3.5. *Polinom $p(x) = x^2 - x + 2$ ima v zaporedju koeficientov 2, -1, 1 dve spremembi predznaka, vendar nima pozitivnih ničel (sploh nima realnih ničel).*

Oglejmo si sedaj nekaj splošnih rezultatov, ki se nanašajo na zaporedje (3.4) in $V(\boldsymbol{a})$. Najprej opazimo naslednje.

LEMA 3.3. *Prvi in zadnji neničelni element v zaporedju* (3.4) *imata isti (nasprotni) predznak natanko tedaj, ko je $V(\boldsymbol{a})$ sodo (liho) število.*

Iz prejšnje leme neposredno sledi naslednji rezultat.

LEMA 3.4. *Naj bo $r_0, r_1, \ldots, r_{n-1}$ zaporedje pozitivnih števil. Definirajmo zaporedje $V(\boldsymbol{b}) = (b_j)_{j=0}^{n}$ takole:*

$$\begin{aligned} b_0 &= a_0, \\ b_j &= a_j + r_{j-1}\, b_{j-1}, \quad j = 1, 2, \ldots, n. \end{aligned} \tag{3.10}$$

Če so a_0, a_n in b_n vsi neničelni in je $V(\boldsymbol{a}) = V(\boldsymbol{b})$, sta predznaka števil a_n in b_n enaka.

DOKAZ. Ker je $V(\boldsymbol{a}) = V(\boldsymbol{b})$, sta $V(\boldsymbol{a})$ in $V(\boldsymbol{b})$ seveda iste parnosti, zato sta po prejšnji lemi produkta $a_0\, a_n$ in $b_0\, b_n$ istega predznaka. Ker je po definiciji $a_0 = b_0$ in po privzetku $a_0\, a_n\, b_n \neq 0$, morata biti a_n in b_n istega predznaka. □

Tudi naslednji razmislek je prepost in ga prepuščamo bralcu.

LEMA 3.5. *Naj bo* $\boldsymbol{a} = (a_0, a_1, \ldots, a_n)$ *in* $\widetilde{\boldsymbol{a}} = (a_0, a_1, \ldots, a_n, a_{n+1})$. *Potem je* $V(\boldsymbol{a}) \leq V(\widetilde{\boldsymbol{a}}) \leq V(\boldsymbol{a}) + 1$.

Sedaj pa bomo z indukcijo dokazali malce globji rezultat.

LEMA 3.6. *Naj bo zaporedje* $\boldsymbol{b} = (b_0, b_1, \ldots, b_n)$ *definirano z* (3.10) *kot v lemi 3.4. Potem je* $V(\boldsymbol{b}) \leq V(\boldsymbol{a})$. *Če sta števili* $a_0\, a_n \neq 0$ *in* $b_n = 0$, *pa je* $V(\boldsymbol{b}) < V(\boldsymbol{a})$.

DOKAZ. Naj bo $n = 1$. Potem je lahko $V(\boldsymbol{a})$ le 0 ali 1, odvisno od tega ali je produkt $a_0\, a_1$ nenegativen ali negativen. Iz definicije zaporedja $\boldsymbol{b}$ sledi $b_1\, b_0 = a_1\, a_0 + r_0\, a_0^2$. Če je produkt $a_0\, a_1$ nenegativen, je tak tudi produkt $b_1\, b_0$ in število sprememb predznaka je v obeh zaporedjih 0. V primeru, da je $a_0 \neq 0$, je $b_1\, b_0 > 0$ in zato b_1 ne more biti 0. Če je produkt $a_0\, a_1$ negativen, je $V(\boldsymbol{a}) = 1 \geq V(\boldsymbol{b})$ in $V(\boldsymbol{a}) > V(\boldsymbol{b})$ v primeru, ko je $b_1 = 0$.
Predpostavimo sedaj, da lema drži za vse pare zaporedij dolžine $n + 1$, ki zadoščajo predpostavkam. Izberimo dve zaporedji $\boldsymbol{a} = (a_0, a_1, \ldots, a_{n+1})$ in $\boldsymbol{b} = (b_0, b_1, \ldots, b_{n+1})$, kjer so členi zaporedja $\boldsymbol{b}$ definirani z rekurzijo (3.10).
Če je $a_0 = 0$, je tudi $b_0 = 0$, zato imata zaporedji $a_1, a_2, \ldots, a_{n+1}$ in $b_1, b_2, \ldots, b_{n+1}$ enako število sprememb predznaka kot zaporednji $\boldsymbol{a}$ in $\boldsymbol{b}$ ter zadoščata pogojem v lemi. Rezultat leme tedaj sledi iz indukcijske predpostavke.
Če je $a_j = 0$, za nek $j > 0$, potem je $b_j = a_j + r_{j-1}\, b_{j-1}$ istega znaka kot b_{j-1}. Torej lahko iz zaporedja $\boldsymbol{a}$ brišemo a_j, iz zaporedja $\boldsymbol{b}$ pa b_j, ne da bi spremenili število sprememb predznaka v enem ali drugem zaporedju. Še več, novonastalo zaporedje $b_0, b_1, \ldots, b_{j-1}, b_{j+1}, \ldots, b_{n+1}$ je ponovno dobljeno na podlagi rekurzije (3.10), saj je $b_{j+1} = a_{j+1} + r_j\, b_j = a_{j+1} + r_j\, r_{j-1}\, b_{j-1}$. Zato rezultat ponovno sledi iz indukcijske predpostavke.
Oglejmo si še primer, ko so vsa števila a_j, $j = 0, 1, \ldots, n + 1$, neničelna.
Najprej opazimo, da je

$$V(b_0, b_1, \ldots, b_n) \leq V(a_0, a_1, \ldots, a_n) \leq V(a_0, a_1, \ldots, a_n, a_{n+1}).$$

Prva neenakost sledi iz indukcijske predpostavke, druga pa iz leme 3.5. Naj bo $b_{n+1} = 0$. Po indukcijski predpostavki je

$$V(b_0, b_1, \ldots, b_n) \leq V(a_0, a_1, \ldots, a_n).$$

Če je $V(b_0, b_1, \ldots, b_n) < (a_0, a_1, \ldots, a_n)$, je tudi $V(\boldsymbol{b}) < V(\boldsymbol{a})$. Če pa je $V(b_0, b_1, \ldots, b_n) = V(a_0, a_1, \ldots, a_n)$, je po indukcijski predpostavki $b_n \neq 0$ in ima po lemi 3.4 enak predznak kot a_n. Toda potem iz $0 = b_{n+1} = a_{n+1} + r_n\, b_n$ sledi, da imata a_{n+1} in b_n različen predznak, zato je $V(\boldsymbol{b}) < V(\boldsymbol{a}$.
Ostane še primer, ko je $b_{n+1} \neq 0$. Po indukcijski predpostavki je ponovno

$V(b_0, b_1, \ldots, b_n) \leq V(a_0, a_1, \ldots, a_n)$. Če je neenakost stroga, je lema dokazana, saj je tedaj v vsakem primeru $V(\boldsymbol{b}) \leq V(\boldsymbol{a})$. Privzemimo, da je torej $V(b_0, b_1, \ldots, b_n) = V(a_0, a_1, \ldots, a_n)$. Dokazati moramo, da je tudi v tem primeru $V(\boldsymbol{b}) \leq V(\boldsymbol{a})$. Privzemimo nasprotno, torej $V(\boldsymbol{b}) > V(\boldsymbol{a})$. Torej je $b_n\, b_{n+1} < 0$ in $a_n\, a_{n+1} > 0$. Števili a_n in b_n imata enak predznak, ponovno po lemi 3.4. Toda potem je po privzetku

$$b_n\, b_{n+1} = b_n\, a_{n+1} + b_n^2\, r_n < 0,$$

torej tudi $a_{n+1}\, b_n < 0$ in posledično $a_{n+1}\, a_n < 0$, kar je protislovje. Izrek je dokončno dokazan. □

Sedaj bomo pravkar izpeljane rezultate uporabili za določanje števila pozitivnih ničel polinoma $p(x) = a_n\, x^n + \cdots a_1\, x + a_0$. Najprej dokažimo naslednjo lemo.

LEMA 3.7. *Naj bo $a_0\, a_n \neq 0$. Potem ima polinom p sodo (liho) število pozitivnih ničel, če je $a_0\, a_n > 0$ ($a_0\, a_n < 0$).*

DOKAZ. Opazimo, da ima polinom $q(x) = x^n + c_{n-1}\, x^{n-1} + \cdots + c_1\, x + c_0$, kjer je $c_i = a_i/a_n$, $i = 0, 1, \ldots, n$, iste ničle kot p. Predznak c_0 je isti kot predznak $a_0\, a_n$, saj je $c_0 = (a_0\, a_n)/a_n^2$. Obenem je $q(0) = c_0$ in $q(x) > 0$ za $x > M$, kjer je M neko dovolj veliko število. To pomeni, da vse pozitivne ničle polinoma q ležijo na intervalu $I = (0, M)$. Zlahka se prepičamo, da je na I liho mnogo ničel, če je $c_0 < 0$, in sodo mnogo ničel, če je $c_0 > 0$. □

Sedaj lahko dokažemo glavni izrek tega poglavja.

IZREK 3.3 (Descartesovo pravilo predznakov). *Naj bo $p(x) = a_n\, x^n + a_{n-1}\, x^{n-1} + \cdots + a_1\, x + a_0$ polinom z realnimi koeficienti in τ število pozitivnih ničel polinoma p. Potem je*

$$V(\boldsymbol{a}) - \tau = 2\, k, \quad k \in \mathbb{N}.$$

DOKAZ. Brez škode za splošnost lahko predpostavimo, da sta a_0 in a_n neničelna (sicer se stopnja polinoma zmanjša, ali pa izločimo (večkratno) ničlo pri 0). Prav tako hitro vidimo, da je

$$\hat{p}(1/x) = \frac{p(x)}{x^n},$$

kjer je

$$\hat{p}(x) = a_0\, x^n + a_1\, x^{n-1} + \cdots + a_{n-1}\, x + a_n.$$

Ker imata p in $\hat{p}$ enako število pozitivnih ničel in je $V(a_0, a_1, \ldots, a_n) = V(a_n, a_{n-1}, \ldots, a_1, a_0)$, lahko izrek dokažemo za $\hat{p}$.

Naj bo ρ pozitivna ničla polinoma $\hat{p}$. Potem je $\hat{p}(x) = (x-\rho)q(x)$, kjer je $q(x) = b_0\,x^{n-1} + b_1\,x^{n-2} + \cdots + b_{n-2}\,x + b_{n-1}$ in se b_i izražajo kot

$$\begin{aligned} b_0 &= 0, \\ b_j &= a_j + \rho\,b_{j-1}, \quad j = 1, 2, \ldots, n-1, \\ b_n &= 0. \end{aligned}$$

Po lemi 3.6 (vzamemo $r_j \equiv \rho$) je $V(\boldsymbol{b}) \leq V(\boldsymbol{a}) - 1$. Po τ korakih dobimo $0 \leq V(\boldsymbol{a}) - \tau$, oziroma $V(\boldsymbol{a}) \geq \tau$. Toda kriterij za sodost ali lihost $V(\boldsymbol{a})$ in τ je po lemah 3.3 in 3.7 isti, zato je nujna razlika sodo število in izrek je dokazan. □

Kaj pa število negativnih ničel polinoma? S preprostim trikom lahko ta problem prevedemo na določanje števila pozitivnih ničel ustreznega polinoma. Opazimo namreč, da je število negativnih ničel polinoma $p(x) = a_n\,x^n + \cdots + a_1\,x + a_0$ enako število pozitivnih ničel polinoma $p(-x) = (-1)^n\,a_n\,x^n + \cdots + (-1)\,a_1 + a_0$. Zanj pa lahko uporabimo Descartesovo pravilo predznakov.

Primer 3.6. *Locirajmo število ničel polinoma $p(x) = x^4 - 2\,x^3 - x^2 - 6$ glede na njihov predznak. Število sprememb predznaka v zaporedju $-6, 0, -1, -2, 1$ je 1, torej ima p natanko eno pozitivno ničlo. Polinom $q(x) = p(-x) = x^4 + 2\,x^3 - x^2 - 6$ ima v zaporedju koeficientov $-6, 0, -1, 2, 1$ eno spremembo predznaka, zato ima q natanko eno pozitivno ničlo, torej ima p natanko eno negativno ničlo. Zaključimo lahko, da ima p natanko eno pozitivno in natanko eno negativno ničlo ter dve konjugirano kompleksni ničli.*

3.3 Meje za ničle kompleksnega polinoma

V tem razdelku si bomo ogledali še nekaj rezultatov, ki nam pomagajo pri lociranju kompleksnih ničel kompleksnega polinoma. Naj bo torej

$$p(z) = a_n\,z^n + a_{n-1}\,z^{n-1} + \cdots + a_1\,z_1 + a_0, \quad a_j \in \mathbb{C},\ j = 0, 1, \ldots, n,$$

polinom s kompleksnimi koeficienti. Poskusili bomo določiti območje $\mathcal{D} \subset \mathbb{C}$, ki vsebuje vse (ali predpisano število) kompleksnih ničel polinoma p. Pri tem bomo vztrajali pri zahtevi, da $\mathcal{D}$ opišemo kot funkcijo koeficientov a_j, $j = 0, 1, \ldots, n$. Problem je ekvivalenten iskanju domene $\mathcal{D} \subset \mathbb{C}$, za katero je $p(z) \neq 0$, $z \in \mathcal{D}$. Definirajmo najprej enega od osnovnih pojmov, *polmer vsebovanosti*.

DEFINICIJA 3.2. *Naj bo $p \in \mathbb{C}[z]$ polinom stopnje n in $z_j \in \mathbb{C}$, $j = 1, 2, \ldots, n$, njegove ničle. Definirajmo*

$$r(p) := \max_{1 \le j \le n} \{|z_j|\}.$$

Pozitivnemu številu r, za katerega je $r(p) \le r$, rečemo radij vsebovanosti polinoma p.

Očitno velja, da so vse ničle polinoma p vsenovane v disku $|z| \le r$, kjer je r poljubni polmer vsebovanosti.
Prvi rezultat, ki določa radij vsebovanosti kot funkcijo koeficientov polinoma p je naslednji.

IZREK 3.4. *Vse ničle nekonstantnega polinoma $p(z) = \sum_{j=0}^{n} a_j z^j$, ki nima ničle pri $z = 0$, so vsebovane v disku $|z| \le \zeta$, kjer je ζ enolična pozitivna rešitev enačbe*

$$|a_n| z^n = \sum_{j=0}^{n-1} |a_j| z^j. \tag{3.11}$$

DOKAZ. Po Descartesovem pravilu predznakov koeficienti polinoma

$$\hat{p}(z) = |a_n| z^n - \sum_{j=0}^{n-1} |a_j| z^j$$

natanko enkrat spremenijo predznak. Torej ima $\hat{p}$ natanko eno pozitivno ničlo ζ, ki je ravno rešitev enačbe (3.11). Naj bo $z \in \mathbb{C}$, $|z| > \zeta$. Potem je

$$\begin{aligned} |p(z)| &= \left|a_n z^n - (-a_{n-1} z^{n-1} - \cdots - a_1 z - a_0)\right| \\ &\ge |a_n| |z|^n - \left(|a_{n-1}| |z|^{n-1} + \cdots + |a_1| |z| + |a_0|\right) > 0. \end{aligned}$$

Torej je $p(z) \neq 0$ in zato $r(p) \le \zeta$. □

Eksplicitno polmer vsebovanosti podaja naslednji izrek.

IZREK 3.5. *Naj bodo $\lambda_j \in (0, \infty)$, $j = 1, 2, \ldots, n$, pozitivna realna števila za katera je*

$$\frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \cdots + \frac{1}{\lambda_n} = 1.$$

Potem je število

$$\max_{1 \le k \le n} \left(\lambda_k \left| \frac{a_{n-k}}{a_n} \right| \right)^{\frac{1}{k}}$$

polmer vsebovanosti za polinom p.

Dokaz. Naj bo

$$\rho = \rho(\lambda_1, \lambda_2, \ldots, \lambda_n) = \max_{1 \le k \le n} \left(\lambda_k \left| \frac{a_{n-k}}{a_n} \right| \right)^{\frac{1}{k}}.$$

Potem je

$$\rho \ge \left(\lambda_k \left| \frac{a_{n-k}}{a_n} \right| \right)^{\frac{1}{k}}, \quad k = 1, 2, \ldots, n.$$

Torej je tudi

$$\frac{1}{\lambda_k} \ge \left| \frac{a_{n-k}\, \rho^{n-k}}{a_n\, \rho^n} \right|, \quad k = 1, 2, \ldots, n.$$

Ker je po predpostavki $\sum_{k=1}^{n} \lambda_k^{-1} = 1$, je torej

$$\sum_{k=1}^{n} \left| \frac{a_{n-k}\, \rho^{n-k}}{a_n\, \rho^n} \right| \le 1,$$

oziroma

$$|a_n| \rho^n \ge \sum_{j=0}^{n-1} |a_j|\, \rho^j.$$

Po izreku 3.4 je število
zgornja meja za polmer vsebovanosti polinoma p, če je

$$|a_n|\, \rho^n \ge |a_{n-1}|\, \rho^{n-1} + \cdots + |a_1|\, rho + |a_0|.$$

Temu pogoju je zadoščeno, če je

$$|a_n|\, \rho^n \ge$$

Po prejšnjem izreku je torej ρ zgornja meja za polmer vsebovanosti polinoma p. Meja je dosežena, če je

$$a_{n-k} = \frac{a_n\, \rho^k}{\lambda_k}, \quad k = 1, 2, \ldots, n.$$

□

Posledica 3.4. *Število*

$$\max_{1 \le k \le n} \left(n \left| \frac{a_{n-k}}{a_n} \right| \right)^{\frac{1}{k}}$$

je polmer vsebovanosti polinoma p.

DOKAZ. V prejšnjem izreku vzamemo $\lambda_1 = \lambda_2 = \cdots = \lambda_n = n$. □

Izraz za polmer vsebovanosti lahko še malo poenostavimo.

POSLEDICA 3.5. *Če je σ enolično določena pozitivna ničla polinoma $q(z) = z^n - z^{n-1} - \cdots - z - 1$, je število*

$$\max_{1\le k\le n} \sigma \left|\frac{a_{n-k}}{a_n}\right|^{\frac{1}{k}}$$

polmer vsebovanosti za p.

DOKAZ. V izreku 3.4 vzamemo $\lambda_k = \sigma^k$, kjer je σ pozitivna rešitev enačbe $\sigma^n = \sigma^{n-1} + \cdots + \sigma + 1$. □ In še ena ocena za polmer vsebovanosti.

IZREK 3.6. *Naj bosta p in q pozitivni števili, za kateri je $1/p + 1/q = 1$. Potem je*

$$r(p) < \left(1 + \left(\sum_{j=0}^{n-1} \left|\frac{a_j}{a_n}\right|^p\right)^{\frac{p}{q}}\right)^{\frac{1}{q}}.$$

Literatura

[1] P. Clement. Congruences for sets of primes. *Amer. Math. Monthly*, 56(1):23–25, 1949.

[2] J. Grasselli. *Elementarna teorija števil.* DMFA-založništvo, Ljubljana, 2009.

[3] A. S. Levin. Descartes' rule of signs–how hard can it be? *Preprint*, 2002.

[4] M. Mignotte and D. Ştefănescu. *Polynomials. An algorithmic approach.* Springer, Singapore, 1999.

[5] J. Mrčun. *Topologija.* DMFA-založništvo, Ljubljana, 2008.

[6] O. Oliveira. The fundamental theorem of algebra: An elementary and direct proof. *Math. Intelligencer*, 33:1–2, 2011.

[7] F. Saidak. A new proof of Euclid's theorem. *Amer. Math. Monthly*, 113(10):937–938, 2006.

[8] I. Vidav. *Algebra.* DMFA, Ljubljana, 1987.

[9] E. Zakrajšek. *Matematično modeliranje.* DMFA-založništvo, Ljubljana, 2004.