Algebra

Ivan Prokić

Fakultet tehničkih nauka, Novi Sad

Predavanje 12

Na prethodnom času

- Trigonometrijski oblik
- Eksponencijalni oblik
- Rotacije u kompleksnoj ravni
- Kompleksni koreni

Polinomi - uvod

Polinomi - podsećanje

Iz sedmog razreda osnovne škole:

- **Konstante ili koeficijenti** su brojevi i simboli koji predstavljaju prozivoljan broj (npr. $0, 1, \sqrt{3}, a$), a **promenljive** su simboli koji mogu biti zamenjeni bilo kojim brojem (npr. t, x, y, z)
- **Monomi** su izrazi sastavljeni od brojeva, promenljivih, kao i izraza dobijenih njihovim množenjem (npr. $3t, at^2, 2at^3$)
- **Polinomi** su algebarski izrazi sastavljeni od konstanti, promenljivih i znakova sabiranja, oduzimanja i množenja (npr. $2(t + t^2), 2t(1 + t)$)
- Svaki polinom se može transformisati u **sređen oblik polinoma** sabiranjem njegovih sličnih monoma (npr. $2t^2 + 2t$). **Stepen polinoma**
- **Sabiranje i množenje polinoma**
- **Rastavljanje polinoma na činioce**

Iz srednje škole:

- **Deljenje polinoma**
- **Koreni kvadratnog polinoma i Vijetove formule**

Polinomi - nastavak

Zaključak: Svaki polinom može se zapisati u sređenom obliku kao

$$a_0 + a_1 t + \ldots + a_{n-1} t^{n-1} + a_n t^n$$

gde je t promenljiva, a $a_0, \ldots, a_n$ su konstante (tj. koeficijenti).

Pitanje: Iz kog skupa su te konstante? Takođe, pošto pri sređivanju polinoma i konstante želimo da sabiramo i množimo, koje osobine operacija na tom skupu želimo da imamo? Prsten? Domen integriteta? Polje?

Odgovor: U osnovnoj i srednjoj školi ste radili sa polinomima nad poljima $(\mathbb{R}, +, \cdot)$ i $(\mathbb{C}, +, \cdot)$. Mi ćemo sada izučavati polinome nad proizvoljnim poljima.

Zašto se baviti polinomima?

- Pomoću polinoma definišemo polinomske funkcije
- Polinomske funkcije su "lepe" jer za računanje koristimo samo osnovne računske operacije
- Mnoge druge funkcije mogu se aproksimirati pomoću polinomskih funkcija (koristeći stepene redove - tek na Matematičkoj analizi 1)
- Polinomske funkcije se pojavljuju u mnogim problemima iz raznih naučnih oblasti (da, i u energetici, elektronici i telekomunikacijama)
- Konkretno ovde, pomoću polinoma nad konačnim poljima $(\mathbb{Z}_p, +, \cdot)$ ćemo kostruisati polja sa p^n elemenata, tj. sva ostala konačna polja (koja se koriste u, npr. kriptografiji i teoriji kodiranja)

Polinomi nad proizvoljnim poljima

Definicija polinoma

Definicija

Neka je $(F, +, \cdot)$ *polje. Skup svih polinoma* $F[t]$ *nad poljem* F *s proizvoljnom promenljivom* t *je dat sa:*

1. *Konstante i promenljiva* t *su polinomi nad poljem* F*;*
2. *Ako su* A *i* B *polinomi nad poljem* F *tada su to i* $(A + B)$ *i* $(A \cdot B)$*;*
3. *Polinomi se dobijaju samo konačnim brojem primena prethodna dva pravila,*

pri čemu su operacije $+$ *i* $\cdot$ *na skupu polinoma* $F[t]$ *takve da su:*

- *asocijativne, komutativne i važi distributivni zakon* $\cdot$ *prema* $+$*;*
- $+$ *i* $\cdot$ *na skupu* F *jesu restrikcije od* $+$ *i* $\cdot$ *na* $F[t]$*;*
- *neutralni elementi su jednica* 1 *i nula* 0 *iz polja* F *(*0 *je neutralni za sabiranje,* 1 *je neutralni za množenje polinoma);*
- *inverzni za polinom* A *u odnosu na sabiranje polinoma je polinom* $-A$*.*

Sređeni oblik polinoma

Iz definicije polinoma direktno sledi:

Teorema

Svaki polinom P iz $F[t]$, sem nula polinoma 0, može se zapisati u obliku $a_0 + a_1 t + \ldots + a_{n-1} t^{n-1} + a_n t^n$, gde su $a_0, \ldots, a_n \in F$ i $a_n \neq 0$.

Napomena

Po definiciji, uzimaćemo da je $t^0 = 1$, tj. jedinica polja F.

Teorema

U skupu $F[t]$ polinomi $a_0 + a_1 t + \ldots + a_{n-1} t^{n-1} + a_n t^n$, sa $a_n \neq 0$, i $b_0 + b_1 t + \ldots + b_{m-1} t^{m-1} + b_m t^m$, sa $b_m \neq 0$, su jednaki akko je $n = m$ i $a_k = b_k$ za sve $k \in \{0, \ldots, n\}$.

Stepen polinoma. Sabiranje polinoma.

Definicija (Stepen polinoma)

Ako je $P = a_0 + a_1 t + \ldots + a_{n-1} t^{n-1} + a_n t^n$, *sa* $a_n \neq 0$, *tada kažemo da je stepen polinoma* P *nenegativan ceo broj* n *i pišemo* $dg(P) = n$.

Napomena

Ako je $P = a_0$ *i* $a_0 \neq 0$ *tada je* $dg(P) = 0$. *Stepen nula polinoma* $P = 0$ *nije definisan.*

Teorema (Sabiranje)

Zbir polinoma $P = a_0 + a_1 t + \ldots + a_{n-1} t^{n-1} + a_n t^n$ *i*
$Q = b_0 + b_1 t + \ldots + b_{m-1} t^{m-1} + b_m t^m$ *jeste polinom* $P + Q$ *čiji su koeficijenti uz* t^k *jednaki sa* $a_k + b_k$ *za sve* k *od* 0 *do* $\max\{n, m\}$.

Primer

Ako su $P = 2 + t + 2t^2$ *i* $Q = 2t + t^2$, *tada je* $P + Q = 2 + (1 + 2)t + (2 + 1)t^2 = 2$, *u* $\mathbb{Z}_3[t]$.

Množenje polinoma

Teorema (Množenje)

Proizvod nenula polinoma $P = a_0 + a_1 t + \ldots + a_{n-1} t^{n-1} + a_n t^n$ *i* $Q = b_0 + b_1 t + \ldots + b_{m-1} t^{m-1} + b_m t^m$ *jeste polinom* PQ *koji je stepena* $dg(PQ) = n + m$ *čiji su koeficijenti uz* t^k *jednaki sa* $a_0 b_k + a_1 b_{k-1} + \ldots + a_{k-1} b_1 + a_k b_0$*, za* $k \in \{0, \ldots, n+m\}$.

Primer

Ako su $P = 2 + t + 2t^2$ *i* $Q = 2t + t^2$*, tada u* $\mathbb{Z}_3[t]$ *važi*

$$PQ = t + (2+2)t^2 + (1+1)t^3 + 2t^4 = t + t^2 + 2t^3 + 2t^4$$

Teorema

Ako su P *i* Q *nenula polinomni nad poljem* F*, tada je* $PQ \neq 0$.

Dokaz

Ako je $dg(P) = n$*, gde je* $a_n \neq 0$ *koeficijent uz* t^n*, i* $dg(Q) = m$*, gde je* $b_m \neq 0$ *koeficijent uz* t^m*, tada je* $a_n b_m$ *koeficijent uz* t^{n+m} *u polinomu* PQ *i važi* $a_n b_m \neq 0$ *jer u polju* F *nema delitelja nule.*

Domen integriteta polinoma

Teorema

Ako je $(F, +, \cdot)$ *polje tada je* $(F[t], +, \cdot)$ *domen integriteta.*

Dokaz

Po definiciji sabiranje i množenje polinoma jesu zatvoreni, asocijativni i komutativni. Takođe, u definiciji polinoma je dato da su neutralni za $+$ *i* $\cdot$ *nula i jednica iz polja* F *i da je inverzni za polinom* $P = a_0 + a_1 t + \ldots + a_{n-1} t^{n-1} + a_n t^n$ *u odnosu na sabiranje* $-P = -a_0 - a_1 t - \ldots - a_{n-1} t^{n-1} - a_n t^n$. *Konačno,* $(F[t], +, \cdot)$ *nema delitelje nule na osnovu prethodne teoreme.*

Napomena

Domen integriteta $(F[t], +, \cdot)$ *nije polje jer ne postoje inverzni elementi u odnosu na množenje. Setimo se drugog domena integriteta koji nije polje:* $(\mathbb{Z}, +, \cdot)$.

Deljenje polinoma

Deljenje u domenu integriteta

Primetimo: Domeni integriteta koji nisu polja su $(\mathbb{Z}, +, \cdot)$ i $(F[t], +, \cdot)$. Ove strukture nemaju inverzne elemente u odnosu na množenje, tj. ne možemo uvek da delimo. Ali, možemo da delimo da ostatkom, da tražimo *NZD* i *NZS*, itd.

Primer

U $(\mathbb{Z}, +, \cdot)$ *i* $(\mathbb{R}[t], +, \cdot)$ *imamo:*

$$
\begin{array}{r}
835 \;:\; 3 \;=\; 278 \\
-6 \\
\hline
235 \\
-21 \\
\hline
25 \\
-24 \\
\hline
1
\end{array}
\qquad\qquad
\begin{array}{r}
(2t^3 - t^2 + 5t \quad) : (t-1) = 2t^2 + t + 6 \\
-(2t^3 - 2t^2) \\
\hline
t^2 + 5t \\
-(t^2 - t) \\
\hline
6t \\
-(6t-6) \\
\hline
6
\end{array}
$$

Deljenje polinoma

Teorema (o deljenju polinoma)

Za svaka dva S i $T \neq 0$ polinoma iz $F[t]$ postoje jedinstveni polinomi Q i R iz $F[t]$ takvi da je

$$S = QT + R \qquad \text{odnosno} \qquad \frac{S}{T} = Q + \frac{R}{T},$$

pri čemu je $R = 0$ ili $dg(R) < dg(T)$.

Dokaz

Razlikujemo tri slučaja:

- $S = 0$: *Tada imamo* $-QT = R$, *pa zbog* $dg(R) < dg(T)$ *mora biti* $Q = 0$ *i* $R = 0$.
- $S \neq 0$ *i* $dg(S) < dg(T)$: *Da bi polinomi sa obe strane znaka jedankosti u* $S = QT + R$ *imali isti stepen mora važiti* $Q = 0$, *odakle je* $R = S$.
- $S \neq 0$ *i* $dg(S) \geq dg(T)$: *Ovo je zapravo jedini zanimljiv slučaj (dokaz na sledećem slajdu).*

Nastavak dokaza 1/2

Slučaj: $S = QT + R$, za $S \neq 0$ i $dg(S) \geq dg(T)$.
Neka je $S = a_0 + \ldots + a_n t^n$ i $T = b_0 + \ldots + b_m t^m$ i $n \geq m$. Tada radimo isti postupak koji smo radili u primeru sa deljenjem dva polinoma: pravimo niz novih polinoma $S_1, \ldots, S_k$, čije vodeće koeficijente obeležavamo sa s_i, sa:

$$
\begin{aligned}
S_1 &= S - a_n b_m^{-1} t^{n-m} T \\
S_2 &= S_1 - s_1 b_m^{-1} t^{dg(S_1)-m} T \\
&\vdots \\
S_k &= S_{k-1} - s_k b_m^{-1} t^{dg(S_{k-1})-m} T
\end{aligned}
$$

Primeti da je $a_n b_m^{-1} t^{n-m} T$ polinom stepena n i da mu je vodeći koeficijent zapravo a_n (vodeći koeficijent od S), te da važi $dg(S) > dg(S_1)$. Iz istog razloga će važiti $dg(S) > dg(S_1) > dg(S_2) > dg(S_3) > \ldots$, pa će za neko k važiti $dg(T) > dg(S_k)$ ili $S_k = 0$.

Nastavak dokaza 1/2

Slučaj: $S = QT + R$, za $S \neq 0$ i $dg(S) \geq dg(T)$.
Neka je $S = a_0 + \ldots + a_n t^n$ i $T = b_0 + \ldots + b_m t^m$ i $n \geq m$. Tada radimo isti postupak koji smo radili u primeru sa deljenjem dva polinoma: pravimo niz novih polinoma $S_1, \ldots, S_k$, čije vodeće koeficijente obeležavamo sa s_i, sa:

$$
\begin{aligned}
S_1 &= S - a_n b_m^{-1} t^{n-m} T \\
S_2 &= S_1 - s_1 b_m^{-1} t^{dg(S_1)-m} T \\
&\vdots \\
S_k &= S_{k-1} - s_k b_m^{-1} t^{dg(S_{k-1})-m} T
\end{aligned}
$$

U primeru sa $S = 2t^3 - t^2 + 5t$ i $T = t - 1$ imamo:

$$
\begin{aligned}
t^2 + 5t &= (2t^3 - t^2 + 5t) - 2t^2(t-1) \\
6t &= (t^2 + 5t) - t(t-1) \\
6 &= 6t - 6(t-1)
\end{aligned}
$$

Primeti da je $a_n b_m^{-1} t^{n-m} T$ polinom stepena n i da mu je vodeći koeficijent zapravo a_n (vodeći koeficijent od S), te da važi $dg(S) > dg(S_1)$. Iz istog razloga će važiti $dg(S) > dg(S_1) > dg(S_2) > dg(S_3) > \ldots$, pa će za neko k važiti $dg(T) > dg(S_k)$ ili $S_k = 0$.

Nastavak dokaza 1/2

Sada iz sistema levo zamenom redom $S_1, \ldots, S_{k-1}$ dobijamo sitem desno:

$$
\begin{aligned}
S_1 &= S - a_n b_m^{-1} t^{n-m} T & \qquad S_1 &= S - a_n b_m^{-1} t^{n-m} T \\
S_2 &= S_1 - s_1 b_m^{-1} t^{dg(S_1)-m} T & \qquad S_2 &= S - (a_n b_m^{-1} t^{n-m} + s_1 b_m^{-1} t^{dg(S_1)-m}) T \\
&\vdots & &\vdots \\
S_k &= S_{k-1} - s_k b_m^{-1} t^{dg(S_{k-1})-m} T & \qquad S_k &= S - (a_n b_m^{-1} t^{n-m} + \ldots + s_k b_m^{-1} t^{dg(S_{k-1})-m}) T
\end{aligned}
$$

Za $R = S_k$ i $Q = a_n b_m^{-1} t^{n-m} + \ldots + s_k b_m^{-1} t^{dg(S_{k-1})-m}$ dobijamo $S = QT + R$ i $dg(R) < dg(T)$. Još samo treba pokazati jedinstvenost ovih Q i R. Pretpostavimo da imamo $S = Q_1 T + R_1$ i $S = Q_2 T + R_2$. Tada dobijamo $(Q_1 - Q_2)T = R_2 - R_1$. Ako bi $Q_1 \neq Q_2$ tada bi sa leve strane imali polinom stepena većeg ili jednakog $dg(T)$, a sa desne stepen bi bio najviše $\max\{dg(R_1), dg(R_2)\}$. Kako je $dg(R_1) < dg(T)$ i $dg(R_2) < dg(T)$ dobili bi kontradikciju (polinomi različitog stepena ne mogu biti jednaki). Odatle zaključujemo $Q_1 = Q_2$, a iz toga sledi i $R_1 = R_2$.

Deljivost polinoma

Podsećanje: Na skupu $\mathbb{Z}$ relacija deli $\mid$ je data sa $t \mid s$ akko $s = qt$. Ako $t \mid s$ tada kažemo da je t faktor od s.

Definicija

Polinom T deli polinom S (oba iz $F[t]$), u oznaci $T \mid S$, ako postoji $Q \in F[t]$ takav da je $S = QT$. Ako $T \mid S$ tada kažemo da je T faktor od S.

Teorema

Neka su $T, S, R \in F[t]$. Tada važi:

1. $T \mid T$ *(Refleksivnost)*
2. $(T \mid S \wedge S \mid R) \Rightarrow T \mid R$ *(Tranzitivnost)*
3. $(T \mid S \wedge S \mid T) \Rightarrow (\exists a \in F) T = aS$ *("Zamalo" simetričnost)*
4. $(T \mid S \wedge T \mid R) \Rightarrow T \mid S + R$
5. $(T \mid S \wedge T \mid R) \Rightarrow T \mid S \cdot R$

Najveći zajednički delilac (NZD)

Podsećanje: Za cele brojeve $NZD(s,t) = w$ akko $w \mid s$ i $w \mid t$ i za svaki w_1 ceo broj takav da $w_1 \mid s$ i $w_1 \mid t$, sledi $w_1 \mid w$.

Definicija

Za polinome $S, T \in F[t]$, imamo $NZD(S,T) = W \in F[t]$ akko

1. $W \mid S$ *i* $W \mid T$ *i*
2. *za svaki* $W_1 \in F[t]$ *takav da* $W_1 \mid S$ *i* $W_1 \mid T$, *sledi* $W_1 \mid W$.

Primer

Za $S = a(t-1)^2(t+2)(t-3)^4 t^7$ *i* $T = b(t+1)^2(t-1)^3 t^5$ *imamo*

$$NZD(S,T) = c(t-1)^2 t^5$$

za bilo koje a, b, c *iz polja nad kojim se polinomi posmatraju.*

Uzajamno prosti polinomi

Podsećanje: Celi brojevi s i t su uzajamno prosti ako je $NZD(s,t) = 1$, tj. nemaju zajedničke (proste) faktore različite od 1 ili -1.

Definicija

Polinomi $S, T \in F[t]$ su **uzajamno prosti** *ako je $NZD(S,T) = a$, gde je $a \in F \backslash \{0\}$. Odnosno, S i T su uzajamno prosti ako nemaju zajedničke faktore različite od konstanti.*

Definicija

Kažemo da je polinom $P \in F[t]$ **normalizovan** *ako mu je vodeći koeficijent jednak jedinici polja F.*

Primer

U $\mathbb{R}[t]$ normalizovan je polinom $x^2 + 1$, dok $2x^2 + 2$ nije.

Euklidov algoritam

Pitanje: Kako proveriti da li su dva polinoma uzajamno prosta? Tj. kako naći *NZD*?
Odgovor: Pomoću Euklidovog algoritma.

Primer

Izračunaj $NZD(45, 106)$.

Izračunaj $NZD(x^3 - 2x + 1, x^2 - 1)$.

Euklidov algoritam

Pitanje: Kako proveriti da li su dva polinoma uzajamno prosta? Tj. kako naći *NZD*?
Odgovor: Pomoću Euklidovog algoritma.

Primer

Izračunaj $NZD(45, 106)$.

$$\underline{106} = 2 \cdot \underline{45} + 16$$

Izračunaj $NZD(x^3 - 2x + 1, x^2 - 1)$.

Euklidov algoritam

Pitanje: Kako proveriti da li su dva polinoma uzajamno prosta? Tj. kako naći NZD?
Odgovor: Pomoću Euklidovog algoritma.

Primer

Izračunaj $NZD(45, 106)$.

$$\begin{aligned} \underline{106} &= 2 \cdot \underline{45} + 16 \\ \underline{45} &= 2 \cdot \underline{16} + 13 \end{aligned}$$

Izračunaj $NZD(x^3 - 2x + 1, x^2 - 1)$.

Euklidov algoritam

Pitanje: Kako proveriti da li su dva polinoma uzajamno prosta? Tj. kako naći *NZD*?
Odgovor: Pomoću Euklidovog algoritma.

Primer

Izračunaj $NZD(45, 106)$.

$$\begin{aligned} \underline{106} &= 2 \cdot \underline{45} + 16 \\ \underline{45} &= 2 \cdot \underline{16} + 13 \\ \underline{16} &= 1 \cdot \underline{13} + 3 \end{aligned}$$

Izračunaj $NZD(x^3 - 2x + 1, x^2 - 1)$.

Euklidov algoritam

Pitanje: Kako proveriti da li su dva polinoma uzajamno prosta? Tj. kako naći *NZD*?
Odgovor: Pomoću Euklidovog algoritma.

Primer

Izračunaj $NZD(45, 106)$.

$$\begin{aligned}
\underline{106} &= 2 \cdot \underline{45} + 16\\
\underline{45} &= 2 \cdot \underline{16} + 13\\
\underline{16} &= 1 \cdot \underline{13} + 3\\
\underline{13} &= 4 \cdot \underline{3} + 1\\
\underline{3} &= 3 \cdot \underline{1} + 0
\end{aligned}$$

$NZD(45, 106) = 1$, *tj. brojevi su uzajamno prosti.*

Izračunaj $NZD(x^3 - 2x + 1, x^2 - 1)$.

Euklidov algoritam

Pitanje: Kako proveriti da li su dva polinoma uzajamno prosta? Tj. kako naći *NZD*?
Odgovor: Pomoću Euklidovog algoritma.

Primer

Izračunaj $NZD(45, 106)$.

$$\begin{array}{rcrcr} \underline{106} & = & 2\cdot\underline{45} & + & 16 \\ \underline{45} & = & 2\cdot\underline{16} & + & 13 \\ \underline{16} & = & 1\cdot\underline{13} & + & 3 \\ \underline{13} & = & 4\cdot\underline{3} & + & 1 \\ \underline{3} & = & 3\cdot\underline{1} & + & 0 \end{array}$$

$NZD(45, 106) = 1$, *tj. brojevi su uzajamno prosti.*

Izračunaj $NZD(x^3 - 2x + 1, x^2 - 1)$.

$$\underline{x^3 - 2x + 1} = x\underline{(x^2 - 1)} + (-x + 1)$$

Euklidov algoritam

Pitanje: Kako proveriti da li su dva polinoma uzajamno prosta? Tj. kako naći NZD?
Odgovor: Pomoću Euklidovog algoritma.

Primer

Izračunaj $NZD(45, 106)$.

$$\begin{array}{rcrcr}
\underline{106} & = & 2 \cdot \underline{45} & + & 16 \\
\underline{45} & = & 2 \cdot \underline{16} & + & 13 \\
\underline{16} & = & 1 \cdot \underline{13} & + & 3 \\
\underline{13} & = & 4 \cdot \underline{3} & + & 1 \\
\underline{3} & = & 3 \cdot \underline{1} & + & 0
\end{array}$$

$NZD(45, 106) = 1$, *tj. brojevi su uzajamno prosti.*

Izračunaj $NZD(x^3 - 2x + 1, x^2 - 1)$.

$$\begin{array}{rcrcr}
\underline{x^3 - 2x + 1} & = & x\underline{(x^2 - 1)} & + & (-x + 1) \\
\underline{x^2 - 1} & = & -x\underline{(-x + 1)} & + & (x - 1)
\end{array}$$

Euklidov algoritam

Pitanje: Kako proveriti da li su dva polinoma uzajamno prosta? Tj. kako naći NZD?
Odgovor: Pomoću Euklidovog algoritma.

Primer

Izračunaj $NZD(45, 106)$.

$$\begin{aligned}
\underline{106} &= 2 \cdot \underline{45} + 16\\
\underline{45} &= 2 \cdot \underline{16} + 13\\
\underline{16} &= 1 \cdot \underline{13} + 3\\
\underline{13} &= 4 \cdot \underline{3} + 1\\
\underline{3} &= 3 \cdot \underline{1} + 0
\end{aligned}$$

$NZD(45, 106) = 1$, *tj. brojevi su uzajamno prosti.*

Izračunaj $NZD(x^3 - 2x + 1, x^2 - 1)$.

$$\begin{aligned}
\underline{x^3 - 2x + 1} &= x\underline{(x^2 - 1)} + (-x + 1)\\
\underline{x^2 - 1} &= -x\underline{(-x + 1)} + (x - 1)\\
\underline{-x + 1} &= (-1)\underline{(x - 1)} + 0
\end{aligned}$$

$NZD(x^3 + 2x + 1, x^2 + 1) = x - 1$, *tj. polinomi nisu uzajamno prosti.*

Jedinstvenost normalizovanog *NZD*-a

Podsećanje: Za $s, t \in \mathbb{N}$ postoji tačno jedan $w \in \mathbb{N}$ takav da je $NZD(s, t) = w$ koji se dobija iz Euklidovog algoritma.

Teorema

Za polinome $S, T \in F[t]$, gde je $S \neq 0$ ili $T \neq 0$, postoji tačno jedan normalizovan $W \in F[t]$ takav da je $NZD(S, T) = W$, koji se dobija iz Euklidovog algoritma.

Dokaz

Razlikujemo tri slučaja:

1. $S = 0$ *i* $T \neq 0$: *tada je normalizovani* $NZD(S, T) = a^{-1}T$, *gde je* a *vodeći koeficijent polinoma* T;
2. $S \neq 0$ *i* $T = 0$: *tada je normalizovani* $NZD(S, T) = b^{-1}S$, *gde je* b *vodeći koeficijent polinoma* S;
3. $S \neq 0$ *i* $T \neq 0$: *ovo je jedini zanimljiv slučaj. Dokaz je na sledećem slajdu.*

Nastavak dokaza (1/2)

Slučaj: $S \neq 0$ i $T \neq 0$. Pretpostavimo da je $dg(S) \geq dg(T)$. Ako primenimo Euklidov algoritam na polinome S i T dobijamo

$$
\begin{array}{rcll}
\underline{S} & = & Q\,\underline{T} & + \quad R_1 \\
\underline{T} & = & Q_1\,\underline{R_1} & + \quad R_2 \\
 & \vdots & & \\
\underline{R_{k-2}} & = & Q_{k-1}\,\underline{R_{k-1}} & + \quad R_k \\
\underline{R_{k-1}} & = & Q_k\,\underline{R_k} &
\end{array}
$$

gde su $R_1, \ldots, R_k$ različiti od nula polinoma. Znamo da je $dg(T) > dg(R_1) > \ldots > dg(R_i) > \ldots$, pa mora postojati $k \in \mathbb{N}$ takav da je $dg(R_k) = 0$ ili da je $R_{k+1} = 0$. Pokažimo da je $NZD(S, T) = R_k$. **Delilac:** Iz poslednje jednakosti u Euklidovom algoritmu imamo da $R_k \mid R_{k-1}$, zatim iz pretposlednje R_k (pošto deli sebe i R_{k-1}) mora da deli i R_{k-2}, itd. Idući kroz jednakosti odozdo ka gore dobijamo iz druge jednakosti da $R_k \mid T$, i na kraju iz prve da $R_k \mid S$.

Nastavak dokaza (2/2)

Najveći delilac: Neka je W_1 takođe zajednički delilac za S i T. Treba pokazati da tada $W_1 \mid R_k$.

$$
\begin{array}{rcrcl}
\underline{S} & = & Q\,\underline{T} & + & R_1 \\
\underline{T} & = & Q_1\,\underline{R_1} & + & R_2 \\
 & \vdots & & & \\
\underline{R_{k-2}} & = & Q_{k-1}\,\underline{R_{k-1}} & + & R_k \\
\underline{R_{k-1}} & = & Q_k\,\underline{R_k} & &
\end{array}
$$

Nastavak dokaza (2/2)

Najveći delilac: Neka je W_1 takođe zajednički delilac za S i T. Treba pokazati da tada $W_1 \mid R_k$.

$$
\begin{array}{rcrcl}
\underline{S} & = & Q\underline{T} & + & R_1 \\
\underline{T} & = & Q_1\underline{R_1} & + & R_2 \\
 & \vdots & & & \\
\underline{R_{k-2}} & = & Q_{k-1}\underline{R_{k-1}} & + & R_k \\
\underline{R_{k-1}} & = & Q_k\underline{R_k} & &
\end{array}
\qquad
\begin{array}{rcrcl}
\underline{S} & - & Q\underline{T} & = & R_1 \\
\underline{T} & - & Q_1\underline{R_1} & = & R_2 \\
 & \vdots & & & \\
\underline{R_{k-2}} & - & Q_{k-1}\underline{R_{k-1}} & = & R_k \\
 & & \underline{R_{k-1}} & = & Q_k\underline{R_k}
\end{array}
$$

Iz ekvivalentnog sistema desno iz prve jednakosti vidimo da ako W_1 deli S i T onda mora da deli i R_1, iz druge da pošto W_1 deli T i R_1 onda mora da deli i R_2. Idući od gore ka dole kroz jednakosti na kraju iz pretposlednje dobijamo da $W_1 \mid R_k$, tj. R_k jeste najveći zajednički delilac polinoma S i T. Jedinstvenost normalizovanog NZD-a $W = a^{-1}R_k$, gde je a vodeći koeficijent od R_k, sledi iz "zamalo" antisimetričnosti.

Šta smo danas radili

- Definicija polinoma nad proizvoljnim poljem
- Domen integriteta polinoma
- Deljenje polinoma
- Uzajamno prosti polinomi i *NZD*
- Euklidov algoritam