Polünoomid. Jaguvus.

(Kui pole öeldud teisiti, siis polünoomid on ringist $\mathbb{R}[x]$ ja R on nullitegureita kommutatiivne ring.)

Ülesanne 1 Jagage polünoom f jäägiga polünoomiga g, kui

1. $f = x^4 - 4x^3 + 5x^2 + x - 1, \quad g = x^2 - 2x - 3;$
2. $f = 4x^3 - 2x + 25, \quad g = x + 2;$
3. $f = 2x^2 - 3x + 1, \quad g = x^3 + 4;$

1.

$$
\begin{array}{rrrrr|l}
x^4 - & 4x^3 + & 5x^2 + & x - & 1 & x^2 - 2x - 3 \\
x^4 - & 2x^3 - & 3x^2 & & & x^2 - 2x + 4 \\
\hline
 & -2x^3 + & 8x^2 + & x - & 1 & \\
 & -2x^3 + & 4x^2 + & 6x & & \\
\hline
 & & 4x^2 - & 5x - & 1 & \\
 & & 4x^2 - & 8x - & 12 & \\
\hline
 & & & 3x + & 11 &
\end{array}
$$

Seega

$$x^4 - 4x^3 + 5x^2 + x - 1 = (x^2 - 2x - 3)(x^2 - 2x + 4) + (3x + 11).$$

Vastus: jagatis on $x^2 - 2x + 4$ ning jääk on $3x + 11$.

Ülesanne 2 Jagage polünoom $2x^4 + x^2 + 2x$ jäägiga polünoomiga $x^2 - 2$ tõlgendades nende polünoomide kordajaid vastavate jäägiklassidena ringist a) $\mathbb{Z}_3$, b) $\mathbb{Z}_5$.

a)

$$
\begin{array}{rrrr|l}
2x^4 + & x^2 + & 2x & & x^2 - 2 \\
2x^4 - & x^2 & & & 2x^2 + 2 \\
\hline
 & 2x^2 + & 2x & & \\
 & 2x^2 & & -1 & \\
\hline
 & & 2x + & 1 &
\end{array}
$$

Vastus: jääk on $2x + 1$ ning jagatis on $2x^2 + 2$.

Ülesanne 3 Milliste a, b ja c väärtuste korral jagub polünoom $x^4 + ax^2 + b$ polünoomiga $x^2 + cx + 1$ ringis $\mathbb{Q}[x]$?

Oletame, et $x^2 + cx + 1$ jagab polünoomi $x^4 + ax^2 + b$. Siis leidub selline polünoom g, millega esimest polünoomi korrutades saame teise. Kuna $\mathbb{Q}[x]$ on nullitegureita, siis polünoomide korrutamisel polünoomide astmed liituvad ja seega g peab olema teise astme polünoom, kusjuures x^2 kordaja peab olema 1. Olgu $g = x^2 + ux + v$. Siis

$$x^4 + ax^2 + b = (x^2 + cx + 1)(x^2 + ux + v) = x^4 + (u + c)x^3 + (v + uc + 1)x^2 + (cv + u)x + v.$$

Seega saame, et a, b, c, u, v peavad rahuldama võrrandisüsteemi

$$
\begin{cases}
u + c &= 0 \\
v + uc + 1 &= a \\
cv + u &= 0 \\
b &= v.
\end{cases}
$$

Järelikult $u = -c$, $a = b - c^2 + 1$ ja $cb - c = 0$. Viimane võrdus annab, et $c(b-1) = 0$. Selle võrduse kehtimiseks on kaks võimalust.

1) $c = 0$. Siis $u = 0$ ja $a = b+1$. Seega saame kolmikud $(b+1, b, 0)$, kus $b \in \mathbb{Q}[x]$. Kontrollime:

$$
\begin{array}{rrrr|l}
x^4 & +\ (b+1)x^2 & + & b & x^2+1 \\ \cline{5-5}
x^4 & +\ \quad x^2 & & & x^2+b \\ \cline{1-4}
 & bx^2 & + & b & \\
 & bx^2 & + & b & \\ \cline{2-4}
 & & & 0 &
\end{array}
.
$$

2) $b = 1$. Siis $v = 1$ ja $a = -c^2 + 2$. Siit saame kolmikud $(-c^2+2, 1, c)$, kus $c \in \mathbb{Q}[x]$. Kontrollime:

$$
\begin{array}{lrrrr|l}
x^4 & & +\ (-c^2+2)x^3 & & +\ 1 & x^2+cx+1 \\ \cline{6-6}
x^4\ + & cx^3\ + & x^2 & & & x^2-cx+1 \\ \cline{1-3}
 & -cx^3 & +\ (-c^2+1)x^2 & & +\ 1 & \\
 & -cx^3\ - & c^2x^2 & -\ cx & & \\ \cline{2-5}
 & & x^2 & +\ cx & +\ 1 & \\
 & & x^2 & +\ cx & +\ 1 & \\ \cline{3-5}
 & & & & +\ 0 &
\end{array}
$$

Vastus: sobivateks kolmikuteks $(a, b, c) \in \mathbb{Q}[x]^3$ on kolmikud $(b+1, b, 0)$, kus $b \in \mathbb{Q}[x]$, ja kolmikud $(-c^2+2, 1, c)$, kus $c \in \mathbb{Q}[x]$.

Ülesanne 4 Milliste a ja b väärtuste korral jagub polünoom $x^4 + a$ polünoomiga $x^2 + bx + 1$ ringis $\mathbb{Q}[x]$?

Ülesanne 5 Kas polünoom $2x + 1$ on pööratav a) ringis $\mathbb{Z}_4[x]$, b) ringis $\mathbb{Z}_5[x]$, c) ringis $\mathbb{Z}[x]$?

a) On, sest

$$(2x+1)(2x+1) = 4x^2 + 4x + 1 = 1.$$

b), c) Ei ole, sest ringid $\mathbb{Z}_5$ ja $\mathbb{Z}[x]$ on nullitegureita.

Ülesanne 6 Leidke kõik ülimalt 2. astme taandumatud polünoomid üle korpuse $\mathbb{Z}_3$.

Ülesanne 7 Tooge näiteid polünoomidest, mille ühine tegur on $x + 1$.

Näiteks polünoomid $(x+1)(x-1)$ ja $(x+1)(x+1)$.

Ülesanne 8 Kasutades Eukleidese algoritmi leidke polünoomide f ja g jaoks sellised polünoomid u ja v, et $uf + vg = \text{SÜT}(f, g)$, kui

1. $f = x^4 + x^3 - 3x^2 - 4x - 1, \quad g = x^3 + x^2 - x - 1$;
2. $f = 4x^4 - 2x^3 - 16x^2 + 5x + 9, \quad g = 2x^3 - x^2 - 5x + 4$.

1. Jagame polünoomi f polünoomiga g :

$$
\begin{array}{rl|l}
f = & x^4 + x^3 - \quad 3x^2 - 4x - 1 & x^3 + x^2 - x - 1 = g \\ \cline{3-3}
 & x^4 + x^3 - \quad x^2 - \ x & x = q_1 \\ \cline{1-2}
 & \qquad -2x^2 - 3x - 1 =: r_1 &
\end{array}
$$

Jagame polünoomi g polünoomiga r_1 korrutades vahetulemusi sobivate nullist erinevate konstantidega:

$$
\begin{array}{rl|l}
g = & x^3 + x^2 - x - 1 & -2x^2 - 3x - 1 = r_1 \\ \cline{3-3}
2g = & 2x^3 + 2x^2 - 2x - 2 & -x; 1 \\
 & 2x^3 + 3x^2 + x & \\ \cline{1-2}
g_1 := & -x^2 - 3x - 2 & \\
2g_1 = & -2x^2 - 6x - 4 & \\
 & -2x^2 - 3x - 1 & \\ \cline{2-2}
r_2 := & -3x - 3 &
\end{array}
$$

Jagame polünoomi r_1 polünoomiga $-\frac{1}{3}r_2$:

$$
\begin{array}{rl|l}
r_1 = & -2x^2 - 3x - 1 & x + 1 = -\frac{1}{3}r_2 \\ \cline{3-3}
 & -2x^2 - 2x & -2x - 1 \\ \cline{1-2}
 & - x - 1 & \\
 & - x - 1 & \\ \cline{2-2}
r_3 := & 0 &
\end{array}
$$

Seega f ja g suurim ühistegur on viimane nullist erinev jääk ehk $-3x-3 = r_2$. Jagamistulemused võib kokku võtta järgmiste võrduste abil:

$$
\begin{aligned}
f &= xg + r_1, \\
2g &= (-x)r_1 + g_1, \\
2g_1 &= r_1 + r_2.
\end{aligned}
$$

Kasutades neid võrdusi saame r_2 avaldada f ja g kaudu:

$$
\begin{aligned}
\text{SÜT}(f,g) &= r_2 = 2g_1 - r_1 = 2(2g + xr_1) - r_1 = 4g + r_1(2x-1) = 4g + (f - xg)(2x-1) \\
&= f(2x-1) + g(-2x^2 + x + 4).
\end{aligned}
$$

Niisiis võime võtta $u = 2x - 1$ ja $v = -2x^2 + x + 4$.

Kontroll:

$$
\begin{aligned}
fu + gv &= (x^4 + x^3 - 3x^2 - 4x - 1)(2x-1) + (x^3 + x^2 - x - 1)(-2x^2 + x + 4) \\
&= 2x^5 - x^4 + 2x^4 - x^3 - 6x^3 + 3x^2 - 8x^2 + 4x - 2x + 1 \\
&\quad -2x^5 + x^4 + 4x^3 - 2x^4 + x^3 + 4x^2 + 2x^3 - x^2 - 4x + 2x^2 - x - 4 \\
&= -3x - 3.
\end{aligned}
$$

Ülesanne 9 *Olgu* $d = \text{SÜT}(f,g)$, $\deg(d) = k$, $\deg(f) = n$ *ja* $\deg(g) = m$ *(*$f, g, d \in K[x]$*). Tõestage, et leiduvad sellised polünoomid* u *ja* v*, et* $\deg(u) \leq m - k - 1$, $\deg(v) \leq n - k - 1$ *ja* $fu + gv = d$.

Teame, et leiduvad polünoomid u' ja v' nii, et $fu' + gv' = d$. Peame näitama, et leiduvad sobivate astmetega polünoomid u ja v nii, et $fu + gv = d$.

Kui $\deg u' < m - k$ ja $\deg v' < n - k$, siis on kõik korras. Oletame üldsust kitsendamata, et $\deg u' \geq m - k$. Suurima ühisteguri definitsiooni põhjal leiduvad sellised polünoomid g_1 ja f_1, et $g = dg_1$ ja $f = df_1$. Jagades polünoomi u' jäägiga polünoomiga g_1 saame sellised polünoomid q ja r, et

$$u' = g_1 q + r \text{ ja } \deg r < \deg g_1 = \deg g - \deg d = m - k.$$

Järelikult

$$d = fu' + gv' = f(g_1 q + r) + gv' = fr + f_1 d g_1 q + gv' = fr + g(f_1 q + v') = fu + gv,$$

kus oleme tähistanud $u := r$ ja $v := f_1 q + v'$. On selge, et $\deg u = \deg r \leq m - k - 1$. Jääb veel näidata, et $\deg v \leq n - k - 1$.

Paneme tähele, et kuna $d \mid f$, siis $\deg d \leq \deg f$ ning seega $\deg gv = \deg(d - fu) = \deg fu$. Järelikult

$$m + \deg v = \deg g + \deg v = \deg gv = \deg fu = \deg f + \deg u < n + m - k.$$

Lahutades selle võrratuse mõlemast poolest m saame $\deg v < n - k$ ehk $\deg v \leq n - k - 1$, mida oligi vaja näidata.

Ülesanne 10 Leidke määramata kordajate meetodil sellised polünoomid u ja v, et $uf + vg = \text{SÜT}(f, g)$, kui a) $f = x^3 + 3x + 3$ ja $g = x^2 - x - 2$, b) $f = x^4$ ja $g = x^3 - 3x^2 + 4$.

Ülesanne 11 Leidke kolmanda astme polünoom, millel on ühekordne juur 2 ja kahekordne juur -1.

Ülesanne 12 Leidke polünoomi

$$f(x) = (4 - 2x - 3x^5)^{1632}(7 - x^2 - 7x^7)^{2002} \in \mathbb{Q}[x]$$

kordajate summa.

Ülesanne 13 Leidke ringis $\mathbb{Q}[x]$ jagatis ja jääk, mis tekivad polünoomi $2x^5 - 5x^3 - 8x$ jagamisel polünoomiga $x + 3$.

Ülesanne 14 Kasutades Horneri skeemi leidke $f(-2 - i)$, kui

$$f(x) = x^5 + (1 + 2i)x^4 - (1 + 3i)x^2 + 7.$$

Ülesanne 15 Kasutades Horneri skeemi leidke polünoomi $f(x) = x^4 + 2x^3 - 3x^2 - 4x + 1$ arendus $x + 1$ astmete järgi.

Ülesanne 16 Kasutades Horneri skeemi tehke kindlaks, mitmekordne juur on -2 polünoomile

$$f(x) = x^5 + 7x^4 + 16x^3 + 8x^2 - 16x - 16.$$

Ülesanne 17 Tõestage, et arv 1 on polünoomi $x^{2n} - nx^{n+1} + nx^{n-1} - 1$, $n \geq 4$, kolmekordne juur.

Ülesanne 18 Leidke a nii, et -1 oleks polünoomi $x^5 - ax^2 - ax + 1$ vähemalt kahekordne juur.

Ülesanne 19 Milliste p, q ja r väärtuste korral jagub polünoom $x^4 + px^3 + qx^2 + r$ polünoomiga $(x - 1)^3$ ringis $\mathbb{R}[x]$?

Ülesanne 20 Tõestage, et polünoomil $f(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots + \frac{x^n}{n!}$ ei ole kordseid juuri.

Ülesanne 21 Eraldage polünoomi $f(x) \in \mathbb{R}[x]$ kordsed tegurid (s.o. leidke polünoom $g(x)$, millel on samad taandumatud tegurid, kui polünoomil $f(x)$, kuid kordsusega 1) ning lahutage see polünoom taandumatute tegurite korrutiseks, kui

1. $f(x) = x^5 - 2x^4 + x^3 - x^2 + 2x - 1$;
2. $f(x) = x^5 - 6x^4 + 16x^3 - 24x^2 + 20x - 8$.

Ülesanne 22 Leidke ülimalt kolmanda astme polünoom $f(x)$ kui on teada tema väärtused muutuja x järgmiste väärtuste korral :

c	0	1	2	3
$f(c)$	1	-1	-3	1

.

Ülesanne 23 Tõestage, et mistahes $a, b, c \in R$ korral

1. $a \mid b \wedge b \mid c \Rightarrow a \mid c$;
2. $a \mid b \wedge a \mid c \Rightarrow a \mid b \pm c$;
3. $a \mid b \Rightarrow a \mid bc$.

Ülesanne 24 Tõestage, et mistahes $a, b, c, u \in R$ korral

a) $\text{SÜT}(a, b) = a \Leftrightarrow a \mid b$;

b) $\text{SÜT}(a + bc, b) = \text{SÜT}(a, b)$;

c) u on pööratav $\Rightarrow \text{SÜT}(au, b) = \text{SÜT}(a, b)$;

d) u on pööratav $\wedge d = \text{SÜT}(a, b) \Rightarrow du = \text{SÜT}(a, b)$.

Ülesanne 25 Leidke arvude 975 ja 645 suurim ühistegur ja vähim ühiskordne a) ringis $\mathbb{Z}$, b) ringis $\mathbb{Q}$.

Vaatleme ringi $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$. Defineerime kujutuse $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{N} \cup \{0\}$ võrdusega

$$N(a + b\sqrt{-5}) := a^2 + 5b^2 = \left|a + b\sqrt{5}i\right|^2.$$

Nimetame seda kujutust *normiks.* Kasutades seda, et kompleksarvude korrutamisel tuleb nende moodulid korrutada saame, et norm säilitab korrutamise:

$$N(z_1z_2) = |z_1z_2|^2 = |z_1|^2 |z_1|^2 = N(z_1)N(z_2) \tag{1}$$

iga $z_1, z_2 \in \mathbb{Z}[\sqrt{-5}]$ korral.

Lisaks sellele, mistahes arvude $z_1, z_2 \in \mathbb{Z}[\sqrt{-5}]$ korral

$$z_1 \mid z_2 \text{ ringis } \mathbb{Z}[\sqrt{-5}] \Longrightarrow N(z_1) \mid N(z_2) \text{ ringis } \mathbb{Z}.$$

Tõepoolest, kui $z_1 \mid z_2$ ringis $\mathbb{Z}[\sqrt{-5}]$, siis leidub selline $w \in \mathbb{Z}[\sqrt{-5}]$, et $z_1w = z_2$. Võrduse (1) põhjal $N(z_1)N(w) = N(z_1w) = N(z_2)$, millest aga järeldub, et $N(z_1) \mid N(z_2)$ ringis $\mathbb{Z}$.

Paneme veel tähele, et

$$U(\mathbb{Z}[\sqrt{-5}]) = \{1, -1\}.$$

Sisalduvus $\{1, -1\} \subseteq U(\mathbb{Z}[\sqrt{-5}])$ on ilmne. Oletame, et z on pööratav. Siis $z \mid 1$ ringis $\mathbb{Z}[\sqrt{-5}]$ ning järelikult $N(z) \mid N(1) = 1$ ringis $\mathbb{Z}$. Ainus mittenegatiivne naturaalarv, mis jagab arvu 1 täisarvude ringis, on 1 ise. Seega $N(z) = 1$. Lihtne on näha, et ringis $\mathbb{Z}[\sqrt{-5}]$,

$$N(z) = 1 \Longleftrightarrow z = 1 \text{ või } z = -1.$$

Seega $z \in \{1, -1\}$ ja $U(\mathbb{Z}[\sqrt{-5}]) \subseteq \{1, -1\}$.

Ülesanne 26 Tõestage, et ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ ei ole faktoriaalne.

Vaatleme arvu 9 ja tema kahte teguriteks lahutust

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

On selge, et elemendid 3 ja $2 \pm \sqrt{-5}$ ei ole assotsieeritud, sest kui nad oleksid assotsieeritud, siis nad peaksid olema kas võrdsed või erinema märgi poolest.

Näitame veel, et kõik need elemendid on taandumatud. Paneme tähele, et kui $z \in \{3, 2 + \sqrt{-5}, 2 - \sqrt{-5}\}$, siis $N(z) = 9$. Oletame, et $z \in \{3, 2 + \sqrt{-5}, 2 - \sqrt{-5}\}$ ja $z = z_1 z_2$, kus $z_1, z_2 \in \mathbb{Z}[\sqrt{-5}]$. Siis

$$9 = N(z) = N(z_1)N(z_2). \tag{2}$$

Kuna ei leidu selliseid arve $a, b \in \mathbb{N} \cup \{0\}$, et $a^2 + 5b^2 = 3$, siis ei saa ühegi $\mathbb{Z}[\sqrt{-5}]$ elemendi norm olla 3. Seega võrdusest (2) järeldub, et kas $N(z_1) = 1$ ja $N(z_2) = 9$ või $N(z_1) = 9$ ja $N(z_2) = 1$. Esimesel juhul on z_1 pööratav ja teisel juhul on z_2 pööratav. Sellega oleme tõestanud, et z on taandumatu.

Ülesanne 27 Kas ring $\mathbb{Z}_8[x]$ on faktoriaalne? Põhjendage!

Ülesanne 28 Tehke kindlaks, kas elementidel a, b ringist $\mathbb{Z}[\sqrt{-5}]$ on olemas suurim ühistegur ja vähim ühiskordne, kui 1) $a = 3, b = 1 + \sqrt{-5}$; 2) $a = 6, b = 3 + 3\sqrt{-5}$; 3) $a = 5, b = 1 + \sqrt{-5}$.

1) Näitame, et $\text{SÜT}(3, 1 + \sqrt{-5}) = 1$. Selleks kontrollime definitsiooni kahte tingimust.

1. Ilmselt $1 \mid 3$ ja $1 \mid 1 + \sqrt{-5}$.

2. Oletame, et $c \mid 3$ ja $c \mid 1 + \sqrt{-5}$, kus $c \in \mathbb{Z}[\sqrt{-5}]$. Siis $N(c) \mid N(3) = 9$ ja $N(c) \mid N(1 + \sqrt{-5}) = 6$ ringis $\mathbb{Z}$. Kuna täisarvude ringis on kõik suurimad ühistegurid olemas, siis suurima ühisteguri definitsiooni põhjal $N(c) \mid \text{SÜT}(9, 6) = 3$. Et arvu 3 ainsad naturaalarvulised jagajad on 1 ja 3, siis saame, et $N(c) = 1$ või $N(c) = 3$. Nagu eespool nägime, on teine võimalus välistatud. Seega $N(c) = 1$, mis tähendab, et $c \in \{1, -1\}$, ning seega $c \mid 1$ ringis $\mathbb{Z}[\sqrt{-5}]$, nagu nõutud.

Näitame nüüd, et ei leidu nende arvude vähimat ühiskordset.

Viited

[1] Kilp, M., Algebra I, Tartu, 1998.