Kevad 2014

Näiteid juurimisest lõplikes korpustes

1. Uurime, kas elemendil $-\mathbf{1}$ leidub ruutjuur korpustes $\mathbb{F}_9 = \mathbb{Z}_3[x]/\langle x^2+1\rangle$ ja $\mathbb{F}_7 = \mathbb{Z}_7$.

Korpuses $\mathbb{F}_9$ leidub elemendil $-\mathbf{1}$ ruutjuur vastavalt loengukonspekti järeldusele 8.20, sest $9 \equiv 1 \pmod 4$. Tõepoolest, $-\mathbf{1} = -01 = 02 = 10^2 = (-10)^2 = 20^2$, sest $[x^2+1] = [0]$ ehk $[x]^2 = -[1]$ ehk $10^2 = -01$.

Sama järelduse põhjal ei saa elemendil $-\mathbf{1}$ olla ruutjuurt korpuses $\mathbb{Z}_7$, sest $7 \equiv 3 \pmod 4$. Järele kontrollides tõepoolest $(\pm 1)^2 \equiv 1 \not\equiv -1$, $(\pm 2)^2 \equiv 4 \not\equiv -1$ ja $(\pm 3)^2 \equiv 9 \equiv 2 \not\equiv -1 \pmod 7$.

2. Leiame teise, komanda ja neljanda astme (primitiivsed) ühejuured korpuses $\mathbb{F}_9 = \mathbb{Z}_3[x]/\langle x^2+1\rangle$.

Korpuse $\mathbb{F}_9$ elementide esitused primitiivse elemendi $a = [x+1] = 11$ astmetena on kokku võetud järgmises tabelis:

Prim. el. aste	polünoom
a	11
a^2	20
a^3	21
a^4	02
a^5	22
a^6	10
a^7	12
a^8	01

Loengukonspekti teoreemi 8.18 osa 1) põhjal on a^k n. astme ühejuur, kui $9-1 = 8 \mid nk$. Seega teise astme ühejuured on kujul a^k, kus $4 \mid k$, ehk $a^4 = 02 = -01$ ja $a^8 = 01$. Primitiivne on neist 02. Kolmanda astme ühejuured on kujul a^k, kus $8|k$, ehk $a^8 = 01$, mis ei ole primitiivne. Neljanda astme ühejuured on kujul a^k, kus $2 \mid k$ ehk $a^2 = 20$, $a^4 = 02$, $a^6 = 10$ ja $a^8 = 01$. Kuna teoreemi 8.18 3) põhjal leidub primitiivne neljanda astme ühejuur (sest $4 \mid 8$), $02^2 = 01$ ja $10^{\frac{4}{2}} = 10^2 = (-10)^2 = 02^2 = 02 \neq 01$, siis 01 ja 02 ei saa olla primitiivsed ning 10 ja 20 on primitiivsed (sest ühejuurte rühma H_4 järk on 4, ja me saame rakendada loengukonspekti järeldust 7.20 kontrollimaks, kas 10 ja 20 on selle moodustajad).

3. Leiame 3. astme juurt omavad elemendid korpuses $\mathbb{F}_{16} = \mathbb{Z}_2[x]/\langle x^4+x+1\rangle$.

Loengukonspekti näite 8.14 põhjal on korpuse $\mathbb{F}_{16}$ elementide esitused primitiivse elemendi $a = [x] = 10$ astmetena kokku võetavad järgmise tabeliga:

Prim. el. aste	polünoom
a	0010
a^2	0100
a^3	1000
a^4	0011
a^5	0110
a^6	1100
a^7	1011
a^8	0101
a^9	1010
a^{10}	0111
a^{11}	1110
a^{12}	1111
a^{13}	1101
a^{14}	1001
a^{15}	0001

Ilmselt omab kolmanda astme juurt iga kolmas element, st. element kujul a^k, kus $3 \mid k$. Selliseid elemente on kokku $\frac{15}{3} = 5$ tükki. Teoreemi 8.18 osa 4) järgi on 3. astme juurt omavaid elemente kokku $\frac{16-1}{(3,16-1)} = \frac{15}{3} = 5$. Seega kõik kolmanda astme juurt omavad elemendid ongi eeltoodud $a^3 = 1000$, $a^6 = 1100$, $a^9 = 1010$, $a^{12} = 1111$ ja $a^{15} = 0001$.

Samas me võime leida kõrvalklassid H_3 järgi, mis annavad meile lisaks kätte ka iga elemendi jaoks tema ruutjuured. Kolmanda astme ühejuured on teoreemi 8.18 osa 1) põhjal kujul a^k, kus $15 \mid 3k$, ehk $5 \mid k$. Järelikult

$$H_3 = 0001 \cdot H_3 = \{a^5 = 0110, a^{10} = 0111, a^{15} = 0001\}.$$

Korrutades hulka H_3 järjest eelnevates etappides leitud kõrvalklassi mitte kuuluvate elementidega (muidu me saaksime ühte kõrvalklassi mitu korda), on ülejäänud kõrvalklassid H_3 järgi

$$0010 \cdot H_3 = a \cdot H_3 = \{a^6 = 1100, a^{11} = 1110, a^{16} = a = 0010\},$$

$$0011 \cdot H_3 = a^4 \cdot H_3 = \{a^9 = 1010, a^{14} = 1001, a^{19} = a^4 = 0010\},$$

$$0100 \cdot H_3 = a^2 \cdot H_3 = \{a^7 = 1011, a^{12} = 1111, a^{17} = a^2 = 0100\}$$

ja

$$0101 \cdot H_3 = a^8 \cdot H_3 = \{a^{13} = 1101, a^{18} = a^3 = 1000, a^{23} = a^8 = 0101\}.$$

Järelikult elemendi $0001^3 = 0001$ kuupjuured on 0110, 0111 ja 0001; elemendi $0010^3 = a^3 = 1000$ kuupjuured on 1100, 1110 ja 0010; elemendi $0011^3 = (a^4)^3 = 1111$ kuupjuured on 1010, 1001 ja 0010; elemendi $0100^3 = (a^2)^3 = 1100$ kuupjuured on 1011, 1111 ja 0100 ning elemendi $0101^3 = (a^8)^3 = a^9 = 1010$ kuupjuured on 1101, 1000 ja 0101.