Arvuteooria

Näidislahendused

Praktikum 10

1 Lahenduse autorid on toimetusele teada

Esiteks kuna $(22, 50) = 2 \neq 1$, siis $22 \notin U(\mathbb{Z}_{50})$, seega ei saa rääkida selle elemendi järgust antud rühmas

$|U(\mathbb{Z}_{50})| = \varphi(50) = \varphi(25) \cdot \varphi(2) = 5^1(5-1) \cdot (2-1) = 20$.

Seega Lagrange'i teoreemi põhjal saab elemendi järguks olla ainult rühma järgu (20) jagaja ehk 1, 2, 4, 5, 10 või 20.

a	a^2	a^4	a^5	a^{10}	a^{20}
21	41	31	1		
23	29	41	43	49	1
27	29	41	7	49	1
43	49	1			

Näeme tabelist, et $\mathrm{ord}(21) = 5$, $\mathrm{ord}(23) = 20$, $\mathrm{ord}(27) = 20$ ja $\mathrm{ord}(43) = 4$.

Seejuures, kuna $\mathrm{ord}(23) = \mathrm{ord}(27) = \varphi(50)$, siis 23 ja 27 on algjuurteks mooduli 50 järgi.

2 Johanna Maria Kirss ja Rainer Bõkov

Kirjeldame alustuseks kaarte segades saadud uusi positsioone. Kui kaart oli parempoolses pakis ehk kui ta oli algselt mingil kohal $i \in \{1, \dots, 39\}$, siis nüüd on ta kohal $2i$. Kui aga kaart oli vasakpoolses pakis ehk kohal $i \in \{40, \dots, 78\}$, siis toimub protsess $40 \to 1$, $41 \to 3$ jne kuni $78 \to 77$. Saame öelda, et vasakpoolse paki kaardi uus positsioon on $2i - 79$. Märkame, et mooduli 79 järgi on mõlema paki korral kaardi uueks asukohaks $2i$.

Jätkates niisugust segamist, saame, et mingi kaardi positsioon on algselt i, siis $2i$, siis $2^2 i$ jne. Pärast m segamist on selle kaardi positsiooniks $2^m i$. Meie otsime, mitme segamise pärast saame tagasi algse järjestuse ehk otsime elemendi 2 järku: vähimat m, mille korral

$$2^m \equiv 1 \pmod{79}.$$

Euleri teoreemi järgi teame, et kindlasti $l = \varphi(79) = 78$ korral $2^l \equiv 1 \pmod{79}$. Lemma 7.6 järgi teame, et kahe järk m peab jagama 78-t. Et 78 =

$2 \cdot 39$ ja $m = 2$ kahe järguks ei sobiks, siis proovime juhtu $m = 39$. Tõesti,

$$2^{39} \equiv 1 \pmod{79}.$$

Järelikult saame algse järjestuse tagasi pärast 39 segamist.

3 Erki Külaots ja Marcus Lõo

Astendame jäägiklassi ringi elemente järjest, kui jõuame tulemuseni, et $x^k \equiv 0 \pmod{32}$, siis teame, et ka $x^{k+1} \equiv 0 \pmod{32}$, seega x pole algjuur. Kui jõuame tulemuseni, et $x^k \equiv 1 \pmod{32}$ ja $k < \varphi(32) = 16$, siis pole ka tegu algjuurega, sest rühmas $U(\mathbb{Z}_{32})$ on $\varphi(32) = 16$ elementi, mis peaks kõik olema võimalik saada kätte algjuurt x astendades, aga kui $x^k \equiv 1 \pmod{32}$, siis $x^{k+1} \equiv x \pmod{32}$ ja saame x-ga korrutades edasi samu elemente, mis varem.

Seega kui $x^k \equiv 1 \pmod{32}$, siis x-i astendades saame kätte kuni k elementi.

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8
0	0						
1	1						
2	4	8	16	0			
3	9	27	17	19	25	11	1
4	16	0					
5	25	29	17	21	9	13	1
6	4	24	16	0			
7	17	23	1				
8	0						
9	17	25	1				
10	4	8	16	0			
11	25	19	17	27	9	3	1
12	16	0					
13	9	21	17	29	25	5	1
14	4	24	16	0			
15	1						
16	0						
17	1						
18	4	8	16	0			
19	9	11	17	3	25	27	1
20	16	0					
21	25	13	17	5	9	29	1
22	4	24	16	0			
23	17	7	1				
24	0						
25	17	9	1				
26	4	8	16	0			
27	25	3	17	11	9	19	1
28	16	0					
29	9	5	17	13	25	21	1
30	4	24	16	0			
31	1						

Kuna iga jäägi korral saime astendades kätte 1 või 0 enne x^{16}, siis moodulis 32 puuduvad algjuured.

4 Lahenduse autorid on toimetusele teada

Teoreemi 7.21 põhjal saame, et moodulite 12 ja 16 järgi pole algjuuri (kuna need pole kujul 2, 4, p^k või $2p^k$) ning teistel on vastavalt

- Kuna kui a on algjuur mooduli 9 järgi, siis $(a, 9) = 1$, siis algjuurteks võivad olla 1, 2, 4, 5, 7. 8.

Kuna algjuure järguks peab olema 6, siis ei sobi 1, 4, 7 ja 8, kuna $1 = 1^1 = 8^2 = 7^3 = 4^3 \pmod 9$. Allesjäänud arvud sobivad ehk nende järk on 6.

Algjuured mooduli 9 järgi: 2 ja 5.

- Kuna kui a on algjuur mooduli 14 järgi , siis $(a, 14) = 1$, siis algjuurteks võivad olla 1, 3, 5, 9, 11, 13.

  Kuna algjuure järguks peab olema 6, siis ei sobi 1, 9, 11 ja 13, kuna $1 = 1^1 = 13^2 = 11^3 = 9^3 \pmod{14}$. Allesjäänud arvud sobivad ehk nende järk on 6.

  Algjuured mooduli 14 järgi: 3 ja 5.

- Kuna kui a on algjuur mooduli 18 järgi, siis $(a, 18) = 1$, siis algjuurteks võivad olla 1, 5, 7, 11, 13, 17.

  Kuna algjuure järguks peab olema 6, siis ei sobi 1, 6, 13 ja 17, kuna $1 = 1^1 = 17^2 = 6^3 = 13^3 \pmod{14}$. Allesjäänud arvud sobivad ehk nende järk on 6.

  Algjuured mooduli 18 järgi: 5 ja 11.

5 Urmas Luhaäär ja Kristjan Kallikivi

Tõestame kõigepealt, et kui a on algjuur mod$p$, siis

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

Lahendame kongruentsi

$$x^2 \equiv 1 \pmod p.$$

Kuna tegemist on ruutpolünoomiga ja lahendame teda korpuses(sest p on algarv), siis on tal maksimaalselt kaks lahendit. Nendeks on null ja üks. Näeme, et kui mingi elemendi ruut on üks, siis ta on kas üks või miinus üks. Elemendi $a^{\frac{p-1}{2}}$ ruut on ilmselt üks. Kuna Ta aga ise ei saa üks olla, sest muidu poleks a algjuur mod$p$, siis on ta miinus üks.
Kuna a on algjuur, siis leidub selline $k > 1$, et

$$a^k \equiv -a \pmod p.$$

Kuna a peab olema arvuga p ühistegurita, võime ta taandada. Saame

$$a^{k-1} \equiv -1 \pmod p.$$

Eelnevalt tõestatu põhjal $k-1 = \frac{p-1}{2}$(vaatame astendajaid nullist arvuni $p-1$). Ehk

$$k = \frac{p+1}{2}.$$

Nüüd seosest $a^k \equiv -a \pmod p$ saame, et $-a$ on algjuur parajasti siis, kui $(k, p-1) = (\frac{p+1}{2}, p-1) = 1$. Viimast avaldist saab teisendada $(\frac{p+1}{2}, p-1) = (\frac{p+1}{2}, 2 \cdot \frac{p-1}{2}) = (\frac{p+1}{2}, 2)$, sest $(\frac{p+1}{2}, \frac{p-1}{2}) = 1$. Seega on $-a$ algjuur, kui

$$\left(\frac{p+1}{2}, 2\right) = 1.$$

Mis on samaväärne sellega, et $p \equiv 1 \pmod 4$.

6 Maret Sõmer ja Mikael Raihhelgauz

Olgu p arvu n^4+1 suvaline paaritu algtegur. Siis kehtib kongruents

$$n^4 + 1 \equiv 0 \mod p,$$
$$n^4 \equiv -1 \mod p.$$

Järelikult $n^8 = (n^4)^2 \equiv (-1)^2 \equiv 1 \mod p$. Siit on ilmne, et n on ringis $\mathbb{Z}_p$ pööratav element, sest võttes $n^{-1} = n^7$, saame $n \cdot n^{-1} = n \cdot n^7 = n^8 \equiv 1 \mod p$. Lemma 7.6 põhjal $\mathrm{ord}(n)|8$ ehk $\mathrm{ord}(n) \in \{1, 2, 4, 8\}$. Seejuures paneme tähele, et $(n^1)^4 = (n^2)^2 = n^4 \equiv -1 \mod p$. Järelikult, kui 1, 2 või 4 on n järk, siis $1 \equiv -1 \mod p$, mis ei kehti ühegi paaritu algarvu p korral. Järelikult $\mathrm{ord}(n) = 8$.
Et 8 on elemendi n järk, siis Lagrange'i teoreemi põhjal 8 jagab rühma $U(\mathbb{Z}_p)$ järku ehk $8|\varphi(p) = p-1$. Niisiis leidub $k \in \mathbb{Z}$, et $8k = p-1$ ehk $p = 8k+1$.

7 Lahenduse autorid on toimetusele teada

Tõestada, et $p \in \mathbb{N}$ on algarv siis ja ainult siis, kui $(p-1)! \equiv -1 \pmod p$.

$p = 2$ korral: $(2-1)! = 1 \equiv -1 \pmod 2$.

Oletame nüüd, et $p \geq 3$.

Kuna $\mathbb{Z}_p$ on korpus, siis igal elemendil on pöördelement. Lagrange'i teoreem ütleb, et ainukesed a väärtused, mille korral $a \equiv a^{-1} \pmod p$ on $a \equiv \pm 1 \pmod p$, sest kongruentsil $a^2 \equiv 1$ saab maksimaalselt olla 2 juurt mooduli p järgi. See tähendab, et arvu $(p-1)!$ tegurid saab järjestada paaridesse (element koos oma pöördelemendiga), kus iga paar on kongruentne ühega mooduli p järgi ning üks paar ($\overline{1}$ ja $\overline{p-1}$) on kongruentne -1 mooduli p järgi.
Näiteks $p = 7$ korral: $6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 1 \cdot 6 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \equiv -1 \cdot 1 \cdot 1 \equiv -1 \pmod 7$.
Teistpidi, teame, et kehtib $(p-1)! \equiv -1 \pmod p$.
Oletame vastuväiteliselt, et p on kordarv ehk $\exists a, b : p = a \cdot, \ a \neq 1 \neq b$.
Teame, et $a \mid (p-1)!$ ja $b \mid (p-1)!$.

Vaatame kahte juhtu:
1) $a \neq b$. Sel juhul kehtib ka $a \cdot \ \mid (p-1)!$ ehk $p \mid (p-1)!$ ehk $(p-1)! \equiv p \cdot c \equiv 0 \not\equiv -1$, tekib vastuolu.
2) $a = b$. Sel juhul teame, et $2a \mid (p-1)!$, sest $2a < a^2$, kui $a > 2$.

$$1 \cdot 2 \cdot \ldots \cdot a \cdot \ldots \cdot 2a \cdot \ldots \cdot p - 1 = (p-1)!$$

Järelikult kehtib ka $a^2 \mid (p-1)!$ ehk $(p-1)! \equiv p \cdot \equiv 0 \not\equiv -1$, tekib vastuolu. Samas jääb üle juht $p = 4$, aga kuna $1 \cdot 2 \cdot 3 = 6 = 2! \not\equiv -1 \pmod 4$, tekib ka seal vastuolu.
Kokkuvõttes saame, et $p \in \mathbb{P}$.

8 Johanna Maria Kirss ja Rainer Bõkov

Olgu antud arv a ja algarv $p > 2$ nii, et a on algjuur mooduli p^2 järgi. Siis

$$a^{p(p-1)} \equiv 1 \pmod{p^2}.$$

Eeldame vastuväiteliselt, et mooduli p järgi leidub mingi arv $1 < k < p-1$, mille korral $a^k \equiv 1 \pmod p$. Siis saame öelda, et leidub mingi $x \in \mathbb{N}$, mille korral $a^k = 1 + px$. Võtame arvu a^k astmesse p. Saame binoomvalemi järgi

$$(a^k)^p = (1+px)^p = 1 + \binom{p}{1}px + \binom{p}{2}(px)^2 + \ldots + \binom{p}{p-1}(px)^{p-1} + (px)^p.$$

Saadud summa igas liidetavas peale esimese on p aste vähemalt kaks - kolmandast liidetavast alates on see ilmne, teises $\binom{p}{1} = p$, seega $\binom{p}{1}px = p^2x$. Seega saame, et leidub mingi y nii, et

$$(a^k)^p = 1 + p^2y \equiv 1 \pmod{p^2}.$$

Kuna $k < p-1$, siis astendaja $kp < p(p-1)$. See aga on vastuolus eeldusega, et a on algjuur mooduli p^2 järgi.