Kevad 2016

Märkusi arvuteooria 10. praktikumi kohta:

A. Üldine märkus elemendi järgu ja algjuureks oleku uurimise kohta: Lagrange'i teoreemist tulenevalt tasub järku otsides kontrollida ainult rühma järgu jagajaid, $U(\mathbb{Z}_n)$ korral arvu $\varphi(n)$ jagajaid. Algjuure korral võimaldab järeldus 7.21 meil veelgi rohkem arvutusi kokku hoida ja vaadelda ainult nn. maksimaalseid jagajaid kujul $\frac{p-1}{q}$, kus q on $p-1$ algtegur.

B. Kommentaare ja tüüpvigu ülesannete kaupa:

1. Vastus: $\operatorname{ord}\overline{7} = 3$, $\operatorname{ord}\overline{11} = 6$ ja tegu on algjuurega, $\operatorname{ord}\overline{17} = 2$, mittepöörataval elemendil $\overline{9}$ järku ei ole.
Järku võib leida lihtsalt järjest arvu $\varphi(18) = 6$ jagajatega astendades. Vähim astendaja, mille korral tulemus on kongruentne ühega, ongi järk. Suuremate arvude korral on abiks lemma 7.3.
Kui te mingis etapis leiate, et $a^k \equiv -1 \pmod{n}$, siis a järk on tegelikult $2k$. See on näiteks algjuureks oleku uurimisel kasulik kontrollvõimalus.
Vigu: ei ole mõtet astendada arvudega 1 (esimest järku on ainult element $\overline{1}$) ja $\varphi(n)$ (Euleri teoreemi kohaselt ALATI $a^{\varphi(n)} \equiv 1 \pmod{n}$). Elemendi järk on ühene, nimelt VÄHIM astendaja, mille korral $a^k \equiv 1 \pmod{n}$. Seetõttu ei ole korrektne kirjutada, et elemendi järk on näiteks $2, 4, 8$ jne. Järk on sel juhul ikkagi ainult 2.

2. Vastus: $39 \cdot k$, $k \in \mathbb{N}$.
Ülesande sai taandada elemendi $\overline{2}$ järgu leidmisele rühmas $U(\mathbb{Z}_{79})$, sest iga segamisega korrutub kaardi järjekorranumber arvuga 2 modulo 79. Seega tekib kongruentside süsteem

$$a \cdot 2^x \equiv a \pmod{79},$$

$a = 1, 2, \ldots, 78$. Kuna $\mathbb{Z}_{79}$ on korpus, siis võib kõigi elementidega a läbi jagada ja alles jääb üksainus kongruents

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

3. Antud ülesandes oli eesmärgiks leida KÕIGI elementide erinevad astmed modulo 20, nt.

$$0, 0^2 = 0, 0^3 = 0, \ldots;$$

$$2, 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 \equiv 12, 2^6 \equiv 4, 2^7 \equiv 8, \ldots;$$
$$13, 13^2 \equiv 9, 13^3 = 17, 13^4 \equiv 1, 13^5 \equiv 13, 13^6 \equiv 9, \ldots.$$

Paljud lahendajad arvutasid välja ainult pööratavate elementide astmed.

4. Vastus: algjuured mooduli 13 järgi on 2,6,7,11;
algjuured mooduli 14 järgi on 3 ja 5;
moodulite 15 ja 16 järgi algjuuri ei leidu;
algjuured mooduli 18 järgi on 5 ja 11.
Otsene lahendusviis on lihtsalt läbi kontrollida, milliste elementide järk on $\varphi(n)$.
Efektiivsem meetod: leida üks algjuur järelduste 7.21 (modulo p), 7.12 (modulo p^2) ja teoreemide 7.15 (modulo p^k,$k > 2$) ning 7.16 (modulo $2p^k$) abil. Kui üks algjuur on leitud, saab ülejäänud algjuurte arvutamiseks kasutada järeldust 7.10.

5. Muutus lahendajate vähesuse tõttu *-ülesandeks.
Täielik lahendus: ilmselt $a \not\equiv 1 \pmod{p}$, sest 1 on algjuur ainult rühmas $U(\mathbb{Z}_2)$. Eelduse kohaselt

$$a^3 - 1 = (a-1)(a^2 + a + 1) \equiv 0 \pmod{p}$$

ja kuna p on algarv, siis meil ei ole nullitegureid ja seega ($a - 1 \not\equiv 0 \pmod{p}$)

$$a^2 + a + 1 \equiv 0 \pmod{p}.$$

Nüüd

$$(a+1)^2 = a^2 + 2a + 1 \equiv a \not\equiv 1 \pmod{p}$$

ja

$$(a+1)^3 = (a+1)(a+1)^2 \equiv a(a+1) = a^2 + a \equiv -1 \not\equiv 1 \pmod{p},$$

sest $p > 2$. Ilmselt $(a+1)^1 \not\equiv 1 \pmod{p}$ (muidu $a \equiv 0 \pmod{p}$ ei oleks algjuur) ja lisaks

$$(a+1)^6 = \left((a+1)^3\right)^2 \equiv (-1)^2 = 1 \pmod{p}.$$

Viimasest kongruentsist saab lemma 7.3 tõttu järeldada, et elemendi $\overline{a+1}$ järk peab olema arvu 6 jagaja, seega kas $1, 2, 3$ või 6. Esimesed kolm varianti oleme me eelnevalt välistanud, seega elemendi $\overline{a+1}$ järk on 6.
Levinumaid vigu: uuriti ka võimalikke järke 4 ja 5; ei põhjendatud, miks $1 \not\equiv -1 \pmod{p}$ ja $\overline{a+1}$ ei ole 1. järku.

6. Siin tuli eelneva ülesandega analoogiliselt tõestada, et $\overline{n}$ järk rühmas $U(\mathbb{Z}_p)$ on 8 (ehk et see ei ole $1, 2$ ega 4). Sellisel juhul Lagrange'i teoreemi tõttu $8 \mid \varphi(p) = p - 1$, mis on samaväärne ülesande väitega.
Millegipärast figureeris osades lahendustes $8^{\varphi(p)}$, mille otstarbekus on selles ülesandes vägagi kaheldav.

7. Antud ülesande lahendas ära ainult üks üliõpilane. Täielik lahendus:
Kui $p \mid a$, siis ilmselt on ainus lahend $x \equiv 0 \pmod{p}$. Kui $p \nmid a$, siis p algarvulisuse tõttu on $\overline{a}$ ja $\overline{x}$ pööratavad ($x \not\equiv 0 \pmod{p}$, muidu kehtiks $a \equiv 0 \pmod{p}$) ja järelikult avaldatavad mingi algjuure c astmetena

$$a \equiv c^l \pmod{p} \quad \text{ja} \quad x \equiv c^k \pmod{p},$$

$k, l \in \mathbb{N}$. Seega meie kongruents saab kuju

$$c^{kn} \equiv c^l \pmod{p} \quad \text{ehk} \quad c^{kn-l} \equiv 1 \pmod{p}.$$

Lemma 7.3 põhjal (algjuure c järk on $\varphi(p) = p - 1$)

$$p - 1 \mid kn - l.$$

Paneme siinjuures tähele, et suurused n ja l on fikseeritud, k aga tundmatu, mille leidmine on samaväärne $x \equiv a^k \pmod{p}$ leidmisega. Seega esialgne kongruents on üheselt lahenduv parajasti siis, kui seda on kongruents

$$nk \equiv l \pmod{p-1}.$$

Viimane on lause 6.2. põhjal tõesti üheselt lahenduv, sest eelduse kohaselt $(p - 1, n) = 1$.
Elementide $\overline{a}$ ja $\overline{x}$ pööratavus on oluline ja seetõttu tuleb juhtu $p \mid a$ eraldi kontrollida.

8. Kui a on algjuur modulo p, siis kõigi pööratavate elemendide korrutis $(p - 1)!$ on mingis järjekorras ekvivalentne korrutisega

$$a^1 \cdot a^2 \cdot \ldots \cdot a^{p-1} = a^{1+2+\ldots+(p-1)} = a^{\frac{p(p-1)}{2}} = \left(a^{\frac{p-1}{2}}\right)^p \equiv (-1)^p = -1 \pmod{p}.$$

Fakt $a^{\frac{p-1}{2}} \equiv (-1) \pmod{p}$ on ära põhjendatud näiteks Euleri kriteeriumi tõestuses, aga esineb mitme praktikumi ülesannetes ja teisteski loengukosnpekti tõestustes. Wilsoni teoreem kehtib muuseas ka algarvu 2 korral, erinevalt paljudest teistest 7. ja 8. peatüki tulemustest.
Levinumaks probleemiks oligi $a^{\frac{p-1}{2}} \equiv (-1) \pmod{p}$ poolik või puuduv tõestus.