Kevad 2014

Märkusi arvuteooria 5. praktikumi kohta:

A. Esiteks, praktikumis esilekerkinud arvamuse kohta, et kõike seda, mida ma loengus räägin, võib vabalt uskuda. Põhimõtteliselt võib, aga ei ole sajaprotsendiliselt soovitatav. Esiteks, suurema osa tulemustest tõestan ma teile ära ja teie ülesanne on mitte lihtsalt tulemuse kehtivust uskuda, vaid ka veenduda, et te saate lahendusest aru ja usute viimast ka ilma mingi administratiivse surveta. Selle mõtteviisi propageerimiseks pakun välja, et annan iga kord ühe lisapunkti, kui

1) te suudate loengus esitatu ümber lükata, s.t. ma olen kusagil vea teinud; see võib põhimõtteliselt juhtuda, aga ei ole eriti tõenäoline;

2) te suudate leida vähemalt 5 kuulajat, kellel on põhjendatud raskusi mingi loengu(konspekti) osa mõistmisega (s.t. te suudate identifitseerida täpsed kohad ja mõttekäigud, millega teil on probleeme, mitte "ma ei saanud mitte millestki aru").

Aga nende tulemuste osas, mida ma otseselt ei tõesta, on kaks võimalust: ma kas ütlen otse välja, et nende tõestusi me siin kursuses ei vaatle (sinna alla käivad ka niiöelda "jutustavad" osad) või ma vihjan, et neid asju ei ole raske ise läbi teha. Viimasel juhul peate te olema võimelised seda tõepoolest tegema ja harilikult mingil kujul juba järgmises praktikumis. Kui teil ei ole selge, millisesse klassi mingi osa loengust kuulub, küsige see juba samas loengus üle.

B. Praktikumis tekkis mõte kasutada praktikumi viimast osa järgmise praktikumi ettevalmistusena, näiteks arutada viimase 15 minuti jooksul neid lahendusvõtteid, mida peaks loengukonspektist ja loengust välja lugema, et ülesanded tehtud saaks. Selline tegevus nõuab teiepoolset aktiivset kaastööd, seega ma arvatavasti küsin edaspidi praktikumi alguses üle, kas teil on järgmise praktikumiga seoses mingeid mõtteid või probleeme tekkinud, mida tasuks arutada. Või mõnikord leian ise mõne näite, mida läbi teha. Aga ilma kaasamõtlemiseta ma lihtsalt seda aega iga kord reserveerima ja ülejäänud lahenduste tempot kiirendama ei hakka.

C. Ülesannete kaupa esines seekord selliseid tüüpvigu:

1. Palju leiti pöördelemente proovimise teel. See on väikese mooduli korral täiesti mõistlik, aga üldiselt peaksite te oskama ka algoritmilisi meetodeid. Nendeks on esiteks Eukleidese algoritm: selleks, et leida $\overline{a}^{-1} \in \mathbb{Z}_n$ piisab leida $x, y \in \mathbb{Z}$ selliselt, et $ax+ny = 1$. Siis $\overline{a}^{-1} = \overline{x}$. Ja teiseks Euleri φ-funktsioon: $\overline{a}^{-1} = \overline{a^{\varphi(n)-1}}$.

2. Seda, et kõik pöördelemendid on leitud saab kontrollida Euleri φ-funktsiooni abil: $|U(\mathbb{Z}_n)| = \varphi(n)$, antud juhul $\varphi(30) = 8$.

3. Null ise EI OLE nullitegur. Ja ülesande lahendamiseks tuli kas kasutada või ise tõestada loengu lause 4: jäägiklassiringi iga nullist erinev element on kas pööratav või nullitegur.

4. Jälle vaja kas kasutada või ise ära tõestada loengukonspekti lause 5.8, mis ütleb, et

$$U(R_1 \times \ldots \times R_n) = U(R_1) \times \ldots U(R_n),$$

antud juhul $U(\mathbb{Z}_3 \times \mathbb{Z}_6) = U(\mathbb{Z}_3) \times U(\mathbb{Z}_6)$.

5. Siin tuli esmalt leida $U(Z_{15})$, loengu lause 4 põhjal on ülenäänud elemendid peale 0 nullitegurid ja teoreemi 4.5 isomorfismi kujutava tabeli abil sai leida siis neile vastavad $\mathbb{Z}_3 \times \mathbb{Z}_5$ pööratavad elemendid ja nullitegurid (esimeste puhul on põhjenduseks lause 4.8, teiste puhul näeb tabeli abil ära, et nende kujutised on nullitegurid). Paljudel juhtudel oli mingi osa eelnevast arutelust vahele jäänud.

6. Siin ei piisa teoreemist 4.5 ja sellest, et $(3, 6) = 3 \neq 1$, kuna teoreem 4.5 ei ole tõestatud tarvilikuna. Selle asemel tuleb kasutada vastuväitelist tõestust, lauset 4.8 (kui ringid on isomorfsed, on seda ka pööratavate elementide rühmad) ja ülesannet 4 (esimeses ringis on 6 ja teises 4 pööratavat elementi).

8. Ülesanne osutus raskemaks, kui oli arvata ja muutus *-ülesandeks. Lahendus on iseenesest lihtne: kuna $\overline{k}^2 = \overline{p-k}^2$ iga $k = 1, 2, \ldots, p-1$ korral, siis hulgas $\{b^2 \mid b \in \mathbb{Z}_p\}$ on rangelt vähem elemente, kui hulgas $\mathbb{Z}_p$ (neid on tegelikult algarvu $p > 2$ korral täpselt $\frac{p+1}{2}$).