Kevad 2014

Märkusi arvuteooria 15. praktikumi kohta:

A. Keskmine tulemus oli madalavõitu, arvestades asjaolu, et hiljemalt umbes kolme nädala pärast tuleb teil kõiki selles praktikumis olnud ülesandeid (ja ka teisi, aga siia oli kordamiseks kogutud enam-vähem esinduslik valik ülesandeid) eksamil lahendada osata.

B. Kommentaare ülesannete kaupa:

1. Lahendusi oli mitmesuguseid, aga üks suhteliselt lihtne variant on selline: Kuna kõik tsüklilised ümberpaigutused on saadavad arvust $\underline{abcdef}$ skeemi

$$\underline{abcdef} \to \underline{bcdefa} \to \underline{cdefab} \to \underline{defabc} \to \underline{efabcd} \to \underline{fabcde}$$

abil, siis piisab, kui me tõestame, et jaguvus arvuga 37 säilib igal sammul. Järelikult on meil vaja tõestada vaid seda, et kui arv $A := \underline{abcdef}$ jagub arvuga 37, siis ka arv $\underline{bcdefa}$ jagub arvuga 37. Avaldame

$$\underline{bcdefa} = \underline{abcdef0} + a - \underline{a000000} = 10A - 999999a.$$

Kuna $37 \mid A$ ja $37 \mid 999999$, siis $37 \mid 10A - 999999a = \underline{bcdefa}$.

2. Üks korduv viga oli see, et leiti, et mingi arv x jagub viiega ja järeldati sellest, et tegu ei saa olla algarvuga. Siin on lisaks vaja veel seda, et $x > 5$, sest 5 on algarv ja jagub viiega.

3. Ülesannet oli võimalik mitmel lihtsamal viisil lahendada, aga üldine ja rohkemates situatsioonides kasulik lahendus on järgmine: arv $a48xy$ jagub arvuga 99 parajasti siis, kui ta jagub arvudega 9 ja 11. Seega tekib meil ühekssa ja üheteistkümnega jaguvuse tunnuste kohaselt kongruentside süsteem

$$\begin{cases} 2+4+8+x+y \equiv 0 \pmod 9 \\ 2-4+8-x+y \equiv 0 \pmod{11} \end{cases} \iff \begin{array}{c} x+y \equiv 4 \pmod 9 \\ -x+y \equiv 5 \pmod{11} \end{array}.$$

Kuna x ja y on kümnendnumbrid, siis $0 \le x+y \le 18$ ja $-9 \le -x+y \le 9$, kust

$$\begin{cases} x+y=4 \quad \text{või} \quad x+y=13 \\ -x+y=5 \quad \text{või} \quad x+y=-6 \end{cases}.$$

Ainuke süsteem nende tekkiva nelja lineaarvõrrandisüsteemi seast, mille lahendid x, y on täisarvud vahemikus $[0, 9]$, on

$$\begin{cases} x + y = 13 \\ -x + y = 5 \end{cases},$$

lahenditega on $x = 4$ ja $y = 9$. Järelikult ainus sobiv 99-ga jaguv arv on 24849.

4. Siin oli kaks probleemi:

1) tuleb kas tõestada, et $U(R_1 \times R_2) = U(R_1) \times U(R_2)$ või viidata lausele 5.6;

1) kui pööratavad tegurid on leitud, siis fakti $(5, 9) = 1$, teoreemi 4.5 ja loengus tõestatud teoreemi, mille kohaselt jäägiklassiringi kõik elemendid on kas pööratavad, nullitegurid või nullelement, saab öelda, et kõik ülejäänud, st. mittepööratavad $\mathbb{Z}_5 \times \mathbb{Z}_9$ elemendid peale $0 = (\overline{0}, \overline{0})$ on nullitegurid.

5. Mitmed lahendajad püüdsid tulemuseni jõuda erinevate $2015 = 5 \cdot 13 \cdot 31$ jagajatega jaguvaid arve välistades. Sellise meetodiga on suhteliselt lihtne eksida. Parem on leida kõik need arvud, mis on väiksemad kui 2015 ja mille suurim ühistegur arvuga 2015 on kas 1, 5 või 13 (suuruselt järgmine 2015 jagaja on juba $5 \cdot 13 > 15$). Selleks võib lause 5.10 kohaselt leida

$$\varphi(2015) + \varphi(\frac{2015}{5}) + \varphi(\frac{2015}{13}) = 1440 + 360 + 120 = 1920.$$

6. Siin oli jälle erinevaid lahendusi, aga kaks kõige kindlamat on rakendada kas Hiina jäägiteoreemi või nn. järkjärgulist lahendamist. Ei tasu lihtsalt valemeid erinevatel viisidel manipuleerida ja loota, et see lahendusena kirja läheb.

7. Lahendusi väga palju ei olnud, ilmselt seetõttu, et siin tuli leida kokku 14 erinevat lahendit (mooduli 135 järgi).

8. Juhtu b) silmas pidades soovitan alati kasutata järkjärgulist algjuurte leidmise meetodit skeemi $p \to p^2 \to p^k \to 2 \cdot p^k$ abil (vt. 10. praktikumi 1. ülesande kommentaari) ja mitte kasutada järeldust 7.20.

11. Esiteks, üldistatud Gaussi ruutvastavusseadus (lause 9.21 3)) annab meile võimaluse vältida arvude teguriteks lahutamist ja algarvulisuse kontrolli.

Seega, kus vähegi võimalik, ärge kasutage lause 9.18 omadusi 2) ja 3). Teiseks, kui te kasutate lauset 9.18, siis on efektiivsem rakendada loengus sõnastatud varianti, kus ruutjäägiks olek toimub vastavalt kongruentsusele mooduli 4 või 8 järgi (teoreemide 9.10, 9.14 ja lause 9.7 3) analoogid). Kolmandaks, kui te näete sümboli $(\frac{a}{n})$ "lugejas" mingi arvu ruutu, nt. $(\frac{ab^2}{n})$, siis juhul $(b, n) = 1$ võib selle ruudu ära jätta (ja kui $(b, n) > 1$, siis $(\frac{a}{n}) = 0$). Neljandaks, põhjendage alati igal sammul, miks mingi Legendre'i või Jacobi sümboli väärtus on just selline, nagu te kirjutate (näiteks märgi muutumine ruutvastavuseadust kasutades). Vigu on lihtne teha ja mina ei saa sel juhul kindel olla, et te tõepoolest oskate nende sümbolite väärtusi leida ning võtan punkte maha. Ja lõpetuseks, parem lugege 14. praktikumi materjalide seas olevat näitefaili.