Kevad 2015

Märkusi arvuteooria 9. praktikumi kohta:

A. Kuna kõik ülesanded on kordavad, siis ma seekord detailidesse ei süvene. Aga soovitan kõigil praktikumiks tegemata jäänud ülesanded üle vaadata, sest vaheeksamile võib vabalt igaüks neist veidi muudetud kujul tulla.

A. Kommentaare ülesannete kaupa:

1. Antud jaguvust sai tõestada nii matemaatilise induktsiooni või avaldise $n^4 - 18n^2 + 17$ tegurdamise ja analüüsimise teel, näiteks eraldades täisruudu $(n^2 - 9)^2$.

2. Siin olid lubatud ka korduvad arvud. Analüüsiks sobis nii arvude a, b, c algteguriteks lahutamine kui tähelepanek, et $10 \mid x \mid 100$ kitsendab a, b, c valiku arvudele $10, 20, 50, 100$. Edasine on juba ebasobivate juhtude välistamine. Õige vastus on , et a, b, c on mingis järjekorras $(10, 20, 50)$, $(10, 10, 100)$, $(10, 20, 100)$, $(10, 50, 100)$, $(10, 100, 100)$, $(20, 20, 50)$, $(20, 50, 50)$, $(20, 50, 100)$.

3. Vaja oli lahendada diofantiline võrrandisüsteem

$$\begin{cases} 600x + 250y + 125z &= 20000 \\ x + y + z &= 100. \end{cases}$$

See taandus diofantilisele võrrandile kujul $ax + by = c$ (võimalikke võrrandeid on kolm tükki, olenevalt sellest, milline tundmatu elimineerida), mille lahenditest tuli välja eraldada positiivsed. Nendeks on

$$(x, y, z) \in \{(5, 41, 54), (10, 22, 68), (15, 3, 82)\}.$$

4. Väga lihtne ülesanne, mida võis lahendada kas aritmeetika põhiteoreemi või Eukleidese lemma abil. Kumbki neist annab, et $p \mid 45$, ehk $p = 3$ või $p = 5$, ja sobib vaid $p = 5$.

5. Siin võis analüüsida eraldi paaris ja paaritut juhtu. Aga on olemas ka ilus alternatiivne lahendus, mille pakkus välja Rasmus:

Olgu suvaline kordarv $n > 11$. Arvud $4, 6, 8$ annavad kolmega jagamisel erineva jäägi, siis peab kehtima üks kolmest

$$n - 4 \equiv 0 \pmod 3$$

$$n - 6 \equiv 0 \pmod 3$$

$$n - 8 \equiv 0 \pmod 3$$

Olgu selleks $a \in \{4, 6, 8\}$. Sellisel juhul

$$n = (n - a) + a$$

ning $n - a$ ja a mõlemad on kordarvud.

6. Vaja oli näidata, et $(x^3 - 1) \cdot x^3 \cdot (x^3 + 1)$ jagub alati $504 = 2^3 \cdot 3^2 \cdot 7$ teguritega 8, 9 ja 7. Kõiki kolme juhtu tuli omaette analüüsida, kasutades arvu x jäägiga jagamist sobiva mooduli järgi.

7. Siin oli võimalikuks probleemiks Fermat' väikese teoreemi kasutuskoha kahe silma vahele jätmine. Muidu tuli lihtsalt järjekindlalt mooduli 29 järgi astendada ja korrutada. Õige vastus on: jäägiks on 6.

8. Vaja oli kasutada isomorfismi $\mathbb{Z}_{20}$ ja $\mathbb{Z}_4 \times \mathbb{Z}_5$ vahel, pööratavuse kriteeriumu ja fakti, et mittepööratavad nullist erinevad elemendid on nullitegurid. Pööratavate elementide arvu saab kontrollida Euleri φ-funktsiooni abil: neid on kokku $\varphi(20) = 8$ tükki.

9. Siin tuli lihtsalt leida

$$\varphi(2016) + \varphi(\frac{2016}{2}) + \varphi(\frac{2016}{3}) + \varphi(\frac{2016}{4}) + \varphi(\frac{2016}{6}) + \varphi(\frac{2016}{7}) +$$
$$\varphi(\frac{2016}{8}) + \varphi(\frac{2016}{9}) + \varphi(\frac{2016}{12}) + \varphi(\frac{2016}{14}) + \varphi(\frac{2016}{16}) = 1692.$$

10. Fermat' väike teoreem (ja lisaks on tarvis analüüsida juhtu $x \equiv 0$, mida mitmed ei teinud) annab, et kõigi täisarvude x korral

$$x^{325} = x^{12 \cdot 27} \cdot x \equiv x \pmod{13}$$

ja

$$x^{325} = x^{18 \cdot 28} \cdot x \equiv x \pmod{19}.$$

Seetõttu on ka kongruentsi $x^{325} \equiv x \pmod{247 = 13 \cdot 19}$ lahenditeks kõik täisarvud.

11. Siin võis lahendada kongruentside süsteemi

$$\begin{cases} x+1 \equiv 0 & (\mathrm{mod}\ 3) \\ x+1 \equiv 0 & (\mathrm{mod}\ 4) \\ x+1 \equiv 0 & (\mathrm{mod}\ 6) \\ x+1 \equiv 0 & (\mathrm{mod}\ 9) \\ x+1 \equiv 0 & (\mathrm{mod}\ 15). \end{cases}$$

Liigsete kongruentside eemaldamise ja Hiina jäägiteoreemi või järk-järgulise lahendamise teel tuleb vastuseks $x \equiv 179 \pmod{180}$. Kui võtta positiivsed 179-st suuremad vastused, siis hakkab liiga palju kaameleid üle jääma, seega vastus on 179 kaamelit (vana beduiini oma on siis 180.). Alternatiivina võib vaadata, et

$$\frac{1}{3}+\frac{1}{4}+\frac{1}{6}+\frac{1}{9}+\frac{2}{15}=\frac{179}{180}$$

ja sealt näha, et vastuseks peab olema 179.

12. Siin tuli lihtsalt rakendada kõrgema astme kongruentside lahendamise teooriat süsteemile

$$\begin{cases} 5x^3-3x^2+7x+3 \equiv 0 & (\mathrm{mod}\ 4), \\ 5x^3-3x^2+7x+3 \equiv 0 & (\mathrm{mod}\ 27). \end{cases}$$

Arvutuste lihtsustamiseks tasus proovimismeetodil leida lahendid kohe mooduli 4, mitte 2 ja siis 2^2 järgi. Neli on lihtsalt niivõrd väike arv, et sellega on mõtet otse läbi proovida. Vastuseks on $x \equiv 7, 11, 15, 61, 65, 69 \pmod{108}$.