Kevad 2016

Märkusi arvuteooria 7. praktikumi kohta:

A. Üks üldine märkus: ärge kirjutage

"on lihtne kontrollida/tõestada/näidata" jne.

Kui see on nii, siis kontrollige või tõestage see tulemus ära. Mul ei ole mõtetelugemise võimeid ja ma ei tea, kas te

- tõesti oskate seda teha, mida väidate lihtne olevat, või
- lihtsalt kirjutate selle fraasi sinna, kus te oma lahenduses kindel ei ole.

B. Kommentaare ja tüüpvigu ülesannete kaupa:

1. Antud ülesandel on kaks lahendit modulo 2016, mille võib kirja panna kujul $x \equiv 604 \pmod{1008}$. Mõned levinumad probleemid:

- kongruentsi mõlema poole läbijagamisel tuleb jagada ka moodulit (nii palju, kui see võimalik on, lause 3.11);
- pöördelemendi leidmisel on esimesed kaks mõistlikku sammu proovimine ja Eukleidese algoritm, muud meetodid on tavaliselt arvutusmahukamad.

2. Õige vastus: $x \equiv 121 \pmod{630}$. Tähele tasub panna järgmisi asjaolusid:

- valemi $\overline{a}^{-1} = \overline{a}^{\varphi(n)-1}$ kasutamine on üldiselt arvutusmahukam, kui Eukleidese algoritm;
- kui mingil elemendil on pöördelement, siis me võime temaga läbi jagada isegi seda pöördelementi teadmata, nt.

  $$7x \equiv 7 \pmod{10} \quad \Longrightarrow \quad x \equiv 1 \pmod{10},$$

  sest $(7, 10) = 1$;
- kui te leiate pöördelemendi, siis te peate kuidagi ka põhjendama, miks teie pakutu pöördelement on (teete läbi Eukleidese algoritmi, korrutate algse elemendiga ja saate $\overline{1}$ vms.).

3. Seda ülesannet sai lahendada nn. järk-järgulise meetodiga, aga lihtsam on järeldada, et kas

$$x \equiv 25 \equiv 1 \pmod 6 \quad \text{ja} \quad x \equiv 5 \pmod 6$$

või

$$x \equiv 15 \equiv 3 \pmod 4 \quad \text{ja} \quad x \equiv 5 \equiv 1 \pmod 4.$$

Mõlemad tulemused on omavahel vastuolus.

4. Antud ülesandes on oluline kasutada nn. tingpiraate, st. kapten ja pootsman annavad kokku 5 lisa-saagiosa. Muuseas tuleb ülesande lahenduvuseks eeldada, et kumbki neist ei saanud ülesande käigus surma. Kokkuvõttes tekib kongruentside süsteem

$$\begin{cases} x \equiv 35 & \pmod{99} \\ x \equiv 20 & \pmod{95} \\ x \equiv 13 & \pmod{91}. \end{cases}$$

See süsteem rahuldab Hiina jäägiteoreemi tingimusi ja lahendiks on $x \equiv 2015 \pmod{855855}$. Arvestades, et aardekirst ei saa mahutada sadu tuhandeid münte, pidi seal algselt olema $2015 + 1 = 2016$ münti ja "päris" piraatide vahel läks jagamisele 2015 münti. Kuna $2015 = 5 \cdot 13 \cdot 31$, siis selle jagajad on

$$1, 5, 13, 31, 5 \cdot 13, 5 \cdot 31, 13 \cdot 31 \text{ ja } 2015.$$

Nendest jagajatest suurim, mis ei ületa viimasel sammul allesjäänud tingpiraatide arvu 91, on 65. Seega varandus jaotati 65 osaks $65 - 5 = 60$ piraadi vahel ja haisöödaks läks $91 - 65 = 86 - 60 = 26$ piraati.

5. Antud ülesandes tekib kongruentside süsteem

$$\begin{cases} x \equiv 1 & \pmod 2 \\ x \equiv 1 & \pmod 4 \\ x \equiv 1 & \pmod 6 \\ x \equiv 1 & \pmod 8 \\ x \equiv 1 & \pmod{10} \\ x \equiv 0 & \pmod{13}. \end{cases}$$

Siin tuleb kas teisendada süsteem HJT rakendamiseks sobivale kujule või lahendada järk-järgult. Esimest on kõige lihtsam teha vähima ühiskordse abil: kui $2, 4, 6, 8, 10$ jagavad kõik arvu $x-1$, siis jagab seda ka $[2, 4, 6, 8, 10] = 120$ (ja vastupidi). Seega on meil samaväärne süsteem

$$\begin{cases} x \equiv 1 & \pmod{120} \\ x \equiv 0 & \pmod{13} \end{cases},$$

mida on lihtne HJT abil lahendada. Vastuseks on $x \equiv 481 \pmod{1560}$.

6. Üks võimalus seda ülesannet lahendada on tegurdada $1001 = 7 \cdot 11 \cdot 13$ ja kasutada HJT süsteemi

$$\begin{cases} 100t \equiv -20000016 & (\text{mod } 7) \\ 100t \equiv -20000016 & (\text{mod } 11) \\ 100t \equiv -20000016 & (\text{mod } 13) \end{cases}$$

jaoks. Selle süsteemi lahendiks on $t \equiv 360 \pmod{1001}$, seega otsitavad arvud on

$$20036016, 20136116, 20236216, \ldots, 20936916.$$

Alternatiivina võib lihtsalt leida 1001 kordse üldkuju

$$\underline{abcde} \cdot 1001 = \underline{abc(a+d)(b+e)de} = \underline{20xyzw16}$$

ja tuletada sealt, et $\underline{yz} = 36$ ning x ja w on suvalised numbrid.

7. Ülesande lahendamiseks saab koostada kongruentside süsteemi

$$\begin{cases} x \equiv 0 & (\text{mod } 2^2) \\ x+2 \equiv 0 & (\text{mod } 3^2) \\ \ldots & \\ x+2(n-1) \equiv 0 & (\text{mod } p_n^2) \end{cases},$$

kus p_i on i-s algarv. HJT garanteerib selle süsteemi lahenduvuse, esimene kongruents selle, et tegu on paarisarvudega ja kõik teised mitteruuduvabaduse (mis on samaväärne võrdusega $\mu(m) = 0$). Algarvud p_i ei pea tingimata olema järjestikused, piisab vaid sellest, et nad oleksid erinevad (ja kuidagi garanteeriksid paarsuse). Nende valikuga oli praktikumis teatud segadus.

8. Muutus *-ülesandeks, mistõttu toon ära täieliku lahenduse. Olgu

$$n = 2^k \cdot n',$$

kus $(2, n') = 1$, st. me eraldame standardkujust välja kõik kahe astmed. Kuna $(2, n') = 1$ ja $(3, 2^k) = 1$, siis leiduvad arvud a' ja b' nii, et $2 \cdot a' \equiv 1 \pmod{n'}$ ja $3 \cdot b' \equiv 1 \pmod{2^k}$. Uuesti $(2, n') = 1$ ja HJT tõttu on kongruentside süsteemid

$$\begin{cases} a \equiv 0 & (\text{mod } 2^k) \\ a \equiv a' & (\text{mod } n') \end{cases} \quad \text{ja} \quad \begin{cases} b \equiv b' & (\text{mod } 2^k) \\ b \equiv 0 & (\text{mod } n') \end{cases}$$

lahenduvad. Olgu nende erilahenditeks a_0 ja b_0. Siis

$$4a_0^2 + 9b_0^2 = (2a_0)^2 + (3b_0)^2 \equiv (2 \cdot 0)^2 + (3 \cdot b')^2 \equiv 1^2 = 1 \pmod{2^k}$$

ja

$$4a_0^2 + 9b_0^2 = (2a_0)^2 + (3b_0)^2 \equiv (2 \cdot a')^2 + (3 \cdot 0)^2 \equiv 1^2 = 1 \pmod{n'}.$$

Järelduse 4.3 tõttu ka

$$4a_0^2 + 9b^2 \equiv 1 \pmod{n},$$

mida oligi vaja tõestada. NB! Eelnevas tõestuses võivad 2^k ja n' olla võrdsed ühega ja arutelu jääb ikkagi kehtima, kuid mõned põhjendused vajavad ülekontrollimist.