Kevad 2014

Märkusi arvuteooria 4. praktikumi kohta:

A. Esiteks, praktikumipunktide keskmine on praeguse seisuga monotoonselt kahanev funktsioon. See ei ole hea märk mulle ega teile. Kui teil on ülesannete lahendamisega probleeme, siis minu töö on teid aidata (kuid mitte kõike teie eest ära teha). Seega rohkem julgust lahendamisel ja tekkivate probleemidega minu poole pöördumisel.

B. Eelnev kehtib eriti kõigi nende aine kuulajate kohta, kelle hetke punktisumma on, ütleme, alla 20. See ei ole eksami suhtes kriitiline piir, aga märgib seda, et teil hakkab järg käest ära minema. See on eriti oluline, sest alates järgmisest praktikumist on materjal veidi keerulisem. Lisaks on veel üks selline võimalik raskusastme tõus vast 9. praktikumi kandis.

C. Käesolevas praktikumis tuli veel kord esile asjaolu, et kui ainult üks kuni kolm inimest võtab vaevaks mingit ülesannet korralikult lahendada, siis nende punktisumma tõuseb, ühe inimese korral kaunis tugevalt.

D. Oma kirjalikud lahendused tuleb mulle saata või anda ENNE praktikumi algust. Võib-olla ma varem ei rõhutanud seda, aga alates järgmisest nädalast ma hilinenud lahendusi lihtsalt ei loe.

E. Kuna vaiksed meeldetuletused ei tundu aitavat, siis sama hakkab kehtima ka mulle saadetavate lahendifailide kohta. Kõik mitte-illustratiivsed elektroonilised lahendused ei tohi ületada 500kB ja seda piiri ületavaid osi ei hakka ma samuti lugema.

F. Mult on küsitud, kuidas arvestatakse *-ülesandeid eksamihindes. Kordan üle, et kõik ülesannete ja *-ülesannete (ja TEX) punktid liidetakse kokku ja võrreldakse kohustuslike ülesannete arvuga. Esimene on igaühel jooksvalt näha oma tulemuste tabeli reas, teine asub sama tabeli ülemises paremas nurgas. Tulemuseks olevat % kasutatakse eksamihinde tõstmiseks vastavalt esimeses loengus kirjeldatud skeemile.

G. Ülesannete kaupa esines järgnevaid tüüpvigu:

2. Siin oli puudu loengukonspekti Lemma 4.2 analoogist, s.t. tuli kas tõestada (või viidata vastavale tulemusele) fakt, et $(a, b) = 1, a \mid c, b \mid c \Rightarrow a \cdot b \mid c$. Samuti tegid paljud liiga sügavat analüüsi kolmega jaguvuse jaoks (vaatlesid

jääke neljaga jagamisel jmt). Piisas tähele panna, et $p^2-1=(p+1)(p-1)$ koosneb kahest järjestikusest paarisarvust, millest üks jagub kolmega, sest p ise ei saa jaguda kolmega.

3*. Tuli välja, et see oli nii raske ülesanne, et talle pidi ühe tärni külge panema. Tegelikult see nii keeruline ka ei olnud. Tuli mingil viisil analüüsida, mida korraga ruuduks ja kuubiks olek annab jääkide osas, mis tekivad kas 4, 6, 9, või 36-ga (kõiki ühes lahenduses vaja ei lähe). Samuti oli abiks tähelepanek, et korraga täisruut ja täiskuup olemisest järeldub kuuendaks astmeks olemine.

4**. Selle ülesande lahendas ära vaid üks inimene ja seega on formaalselt tegu **-ülesandega. Sisuliselt oli aga kogu lahendus tähelepaneku taga, et võttes $a \le b \le c$, siis $c \mid b-a \in \{0,1,\ldots,c-1\}$, kust $b-a=0$ ja lahenditeks sobivad kolmikud (a,a,ka), $k \in \mathbb{N}$, ükskõik millises järjekorras.

5. Paljud kasutasid Fermat' väikest teoreemi. Tegelikult oli ülesanne mõeldud arendama teie oskust arvutada mooduli järgi. Näiteks üks osa ülesande lahendusest võiks välja näha nii:

$$2013^{16} \equiv 7^{16} = 49^8 \equiv (-2)^8 = 4^4 = 16^2 \equiv (-1)^2 = 1 \pmod{17}.$$

Muuseas tuleb siit välja, et arvutuslikult on mugav minna alati absoluutväärtuselt vähimale jäägile, nt. $49 \equiv -2 \pmod{17}$, mitte $49 \equiv 15 \pmod{17}$.

6. Jälle oli puudu Lemma 4.2 analoog. Paljud kasutasid loengus antud jaguvustunnuseid 7 ja 11 jaoks, aga 13 puhul rakendasid hoopis teistsugust tunnust (kolmest viimasest numbrist ja ülejäänud numbritest moodustatud arvude vahe jagub 13-ga). Tegelikult kehtib see tunnus tänu faktile $7 \cdot 11 \cdot 13 = 1001$ ka 7 ja 11 korral. Seega kui te juba alternatiive kasutate, tehke seda arukalt.

7. Sama probleem Lemma 4.2 analoogiga. Mõningat raskust valmistas selle korrektne kirjapanek, et jaguvust seitsmega saab kontrollida 672 "bloki" $\underline{201420142014}$ abil.

8. Ikka probleem Lemma 4.2 analoogiga. Paljudes lahendustes oli puudu põhjendus, miks faktist $\underline{xy} \equiv 31 \pmod{99}$ järeldub $\underline{xy} = 31$.

9**. Oli mitu poolikut lahendust ja üks terviklik, mistõttu tärnide hulk suurenes. Edaspidiseks ütlen vast veel seda, et kui te toetute mingile loenguvälisele faktile, siis te peate ka selle ära tõestama, v.a. need juhud, kui tegu on kas loengus mainitud aga tõestamata väitega või on tegu väga mittetriviaalse väitega, mille tõestus on ülesandest endast tunduvalt raskem. Viimasel juhul tasuks minu käest enne üle küsida, kas seda peab või ei pea tõestama.