Märkusi arvuteooria 3. praktikumi kohta:

A. Kolm üldist märkust:

- tõestusülesannete lahendustes on märgata mitte eriti hästi läbimõeldud arutlusi; soovitan kahtluse korral oma mõttekäiku mulle enne praktikumi tutvustada (enne või pärast loengut on selleks ideaalne aeg);
- jälgige oma jooksvat punktisummat ja (vahe)eksamile pääsemiseks vajalikku miinimumi; kui te juba praegu olete kas piiri lähedal või sellest allpool, tuleks tõsiselt mõelda oma edasise tegevuse peale;
- praktikumis kulus päris palju aega täiesti kasutult; palun tulge edaspidi praktikumi paremini ettevalmistatult ja seadke eesmärgiks lahendusele kulutada mitte rohkem kui 10 minutit koos küsimuste ja parandustega; vastasel korral kulutame mõttetult väärtuslikku praktikumiaega ja te peate terviklikke lahenduskäike lugema (heal juhul) siitsamast tagasisidest.

B. Kommentaare ja tüüpvigu ülesannete kaupa:

1. Eratosthenese sõelaga suuri probleeme ei olnud. Mõned nüansid: alati on vaja selgelt ära öelda, milliste algarvudega me sõelume (siin 2,3,5,7,11 ja 13, sest $17 > \sqrt{250}$). Lisaks tasub tähele panna, et sõelumist on efektiivne viia läbi tabeli kujul, kust on välja jäetud paarisarvud, näiteks nii (optimeeritud Jürgeni variant):

~~175~~	~~177~~	179	181	~~183~~
~~185~~	~~187~~	~~189~~	191	193
~~195~~	197	199	~~201~~	~~203~~
~~205~~	~~207~~	~~209~~	211	~~213~~
~~215~~	~~217~~	~~219~~	~~221~~	223
~~225~~	227	229	~~231~~	233
~~235~~	~~237~~	239	241	~~243~~
~~245~~	~~247~~	~~249~~		

2. Algarvul p on NELI jagajat: 1, -1, p ja $-p$. Siin ülesandes see oluline ei olnud, aga mõnikord võib olla.

Ülesannet sai lahendada, tegurdades n^5-n, aga selle asemel võis ka tähele panna, et $1+n+n^2+n^3+n^4>1$ ja seega $n-1=1, n=2$ ning otsitav algarv on $2^5-1=32$.

3. Siin tuli kindlasti vaadelda juhte

$$1,3,5,7,9; \quad 3,5,7,9,11 \quad \text{ja} \quad 5,7,9,11,13,$$

sest need sisaldavad viiega jaguvat algarvu 5 või kolmega jaguvat algarvu 3. Päris paljud näitasid, et üldiselt on viie järjestikuse arvu seas vähemalt üks kolme kordne, aga piisab tegelikult ka viie kordsest.

4. Lahendada sai siin mitmel viisil: uurida kümnendesitust ja leida $1^4, 3^4, 7^4$ ja 9^4; kasutada Fermat' väikest teoreemi; kasutada kongruentse modulo 10. Alati ei kirjutatud välja, et

$$1^4-1=0,\ 3^4-1=80,\ 7^4-1=2400 \quad \text{ja} \quad 9^4-1=6560.$$

See on vajalik, sest ma ei oska mõtteid lugeda ja ei tea, kas te tegelikult need arvud välja arvutasite või oletasite, et kui ülesandes on öeldud "tõestada", siis need kõik peavad nulliga lõppema ja ei olegi vaja rohkem vaeva näha.

5. Lahenduse skeem oli päris mitmetel üldjoontes olemas, aga detailid kippusid jääma lahti kirjutamata. Lisaks ei piisa ülesande sõnastuses olevast eeldusest, tuleb kasutada samuti kehtivat eeldust, et arvu $5x^2-1$ algtegurid $p \nmid x$ on alati kujul $5k \pm 1$.

Korrektne lahendus: oletame vastuväiteliselt, et $q_1, \ldots, q_n$ on kõik algarvud kujul $5k-1$. Vaatleme arvu

$$a = 5(q_1 \cdot \ldots \cdot q_n)^2 - 1.$$

Aritmeetika põhiteoreemi kohaselt on arvul a algtegur $\mathbb{P} \ni p \mid a$. Mistahes algteguri p korral saame arutleda nii: kui $p \mid q_1 \cdot \ldots \cdot q_n$, siis järelduse 1.12 tõttu leidub $i \in \{1, \ldots, n\}$ nii, et $p = q_i$. Aga sellest järeldub, et

$$p \mid a - 5(q_1 \cdot \ldots \cdot q_n)^2 = -1,$$

mis ei ole p algarvulisuse tõttu võimalik. Järelikult $p \nmid q_1 \cdot \ldots \cdot q_n$ ja seega võttes $x = q_1 \cdot \ldots \cdot q_n$ saame, et p peab olema kujul $5k \pm 1$. Samas, kui kõik arvu a algtegurid on kujul $5k+1$, siis on seda ka nende korrutis ehk a ise, aga a on ilmselt kujul $5k-1$. Seega vähemalt üks a algtegur p on kujul $5k-1$, ehk ta on üks arvudest $q_1, \ldots, q_n$. Kuid siis uuesti

$$p \mid a - 5(q_1 \cdot \ldots \cdot q_n)^2 = -1,$$

vastuolu.

6. Kuna antud ülesande lahendas ära vaid üks üliõpilane, muutus see ÕIS-is toodud skeemi kohaselt **-ülesandeks. Toon siinkohal ära täieliku lahenduse, sest praktikumis jäi selle esitamine viimasele minutile:

Ülesande võib esimese n naturaalarvu summa valemi abil teisendada kujule:

$$\frac{n(n+1)}{2} \mid n! \iff n+1 \in \mathbb{N} \setminus \mathbb{P}.$$

($\Rightarrow$) Oletame vastuväiteliselt, et $n+1 \in \mathbb{P}$. Siis $(n+1) \mid 2n!$, kust järelduse 1.11 tõttu leidub $k \in \{2, 3, \dots, n\}$ nii, et $(n+1) \mid k$. See ei ole aga võimalik, sest $n+1 > k$.

($\Leftarrow$) Olgu $n+1$ kordarv, st. $n = ab$, kus üldisust kitsendamata

$$1 < a \leq b < n+1.$$

Siis on meil kaks võimalust: kas $a < b$ või $a = b$ ja $n+1 = a^2$. Esimesel juhul $b < n$, sest kui $b = n$, siis $n+1 = ab \geq 2n$ ja $n = 1$, mis on vastuolus eeldusega $n > 1$. Seega

$$ab \mid 2(n-1)!,$$

sest $a < b \leq n-1$ esinevad korrutises $(n-1)!$ kahe erineva tegurina. Järelikult kahega jagades ja n-ga korrutades

$$\frac{n(n+1)}{2} = \frac{abn}{2} \mid (n-1)! \cdot n = n!.$$

Kahega võime siin jagada sellepärast, et jaguvusseose mõlemal poolel on paarisarvud.

Teisel juhul aga kas

1. $a = 2$ ja $n = 3$, kust $1+2+3 = 6 \mid 6 = 3!$,
2. või $a > 2$ ja $2a < a^2 - 1 = n+1-1$ (miks?) ehk $2a \leq n-1$.

Viimasel juhul saame eelnevaga analoogiliselt

$$a \cdot 2a \mid 4 \cdot (n-1)!$$

ja tulemust neljaga jagades

$$\frac{n(n+1)}{2} = \frac{n \cdot a^2}{2} \mid (n-1)! \cdot n = n!.$$

7-8. Jäävad järgmise praktikumi algusesse.