Kevad 2015

Märkusi arvuteooria 14. praktikumi kohta:

A. Üldiselt peab ütlema, et Legendre'i ja Jacobi sümbolite leidmise algoritm ei ole enamusel just väga selge. Soovitan veel kord lugeda loengukonspekti näidete osa ja lisaks 2014. aasta 14. praktikumi juures olevat näitefaili.

B. Kommentaare ülesannete kaupa:

1. Kõige suurem probleem, mis siin esile kerkis, oli järjepidev arvude algteguriteks lahutamine, mille ebaefektiivsust võrreldes jäägiga jagamisega ma olen mitmeid kordi rõhutanud. Jacobi sümboli leidmise algoritmi keskne idee on järjest Gaussi ruutvastavusseaduse rakendamine ja peale igat sammu mooduli järgi taandamine.

Veel tüüpvigu: ei saa arvutada (sest need ei ole isegi defineeritud) sümbolitega kujul $\left(\frac{m}{n}\right)$, kus n on paarisarv. Kui te rakendate kas ruutvastavusseadust või mõnda kriteeriumi (näiteks kas 2 või -1 ruutjäägiks oleku kohta), siis neid samme tuleb põhjendada. Euleri kriteeriumi asemel tasub kasutada ikkagi ruutvastavusseadust, näiteks $\left(\frac{5}{3331}\right) \equiv 5^{1665} \pmod{3331}$ ei ole arvutamiseks just mugav, aga $3331 \equiv -1 \pmod 4$ on triviaalne.

Vastuseks pidi tulema $\left(\frac{6791}{3567}\right) = 1$.

2. Tavaliselt jäeti lahendamisel põhjendamata samm $(n, n-2) = 1$, mis lubab meil ruudust vabaneda.
Kontrollvastus: $\left(\frac{n^3}{n-2}\right) = 1$ parajasti siis, kui $n \equiv 1, 3 \pmod 8$.

3. Siin sai vaadelda kahte eri juhtu ($p \equiv \pm 1 \pmod 4$), aga tegelikult annavad mõlemad juhud tulemuseks $\left(\frac{-7}{p}\right) = \left(\frac{p}{7}\right)$. Edasi on juba lihtne järgi proovida, et $p \equiv 1, 2, 4 \pmod 7$.

4. Antud ülesanne oli põhimõtteliselt loengukonspekti märkuse 8.17 tundmise peale. Jälle oli põhjendusi napilt, sealhulgas viited eeltoodud märkusele. Ülesande a) osas lahendeid ei ole, sest vastav Jacobi sümboli väärtus tuleb -1, osas b) on aga (kaks) lahendit, kuna Jacobi sümboli väärtus on 1 ja 217 on algarv (seega on tegu Legendre'i sümboliga). Teises osas sai ruutkongruentsist täisruutu eraldada mitmel erineval moel, seega arvutatav sümbol ei olnud üheselt määratud, küll aga tuli tulemuseks alati 1.

5. Teadaoleva informatsiooni põhjal sai arvutada $\left(\frac{-2a}{n}\right) = -1$, mis märkuse 8.17 kohaselt tähendab kongruentsi mittelahenduvust. Vastupidine ei kehti, näiteks $\left(\frac{2}{21}\right) = 1$, aga $(x+1)^2 \equiv -2 \cdot 2 \pmod{21}$ ei ole lahenduv, sest $\left(\frac{-4}{21}\right) = \left(\frac{-1}{7}\right) = 1$. Terve selle mõttekäiguni ei jõudnud just paljud.

6. Kõige lihtsam lahendus on selline: kuna $p \equiv 1 \pmod 4$, siis $\left(\frac{-1}{p}\right) = 1$. Järelikult kui a on ruutjääk, siis

$$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{a}{p}\right) = \left(\frac{a}{p}\right) = 1$$

ja ka $-a \equiv p - a \pmod p$ on ruutjääk. Kuna $\frac{p-1}{2}$ on paaris, siis me saame igale ruutjäägile vahemikust $1 \leq a \leq \frac{p-1}{2}$ seada vastavusse ruutjäägi $\frac{p-1}{2} < p - a < p$. Selliseid paare on kokku $\frac{p-1}{2}$ tükki ja iga paari elementide summa on p, järelikult kõigi ruutjääkide summa vahemikust $1 \leq a < p$ on

$$\frac{p-1}{2} \cdot p \equiv 0 \pmod p.$$

7. Jälle said *-ülesannete read täiendust, isegi kahetärniülesandega. Näitelahendus: tarvilikkus on ilmne, võtame ühe neist täisruutudest, näiteks $x^2 = a + k_x b > 0$. Siis $a \equiv x^2 \pmod b$ ja a on ruutjääk mooduli b järgi.

Tarvilikkuse jaoks olgu a ruutjääk, st. $a \equiv x^2 \pmod p$ ehk $a = x^2 + kb$ mingi $k \in \mathbb{N}$ korral. Iga $n \in \mathbb{N}$ korral leime

$$z_n := a+(n^2b+2nx-k)b = a-kb+2nxb+(nb)^2 = x^2+2nxb+(nb)^2 = (x+nb)^2.$$

Kuna arv x on võimalik valida positiivne ja $b > 0$, siis piisavalt suure n korral $n^2b + 2nx > k$ ja $n^2b + 2nx - k > 0$. Seega alates sellest indeksist on z_n vaadeldava aritmeetilise jada liige, mis on võrdne täisruuduga. Ilmselt on selliseid täisruute z_n lõpmata palju.
Märkus: kordaja $m = n^2b + 2nx - k$ valik tuleneb võrdusest

$$a + mb = x^2 + (m+k)b = (x+nb)^2.$$

8. Ka see ülesanne sai endale tärni peale. Ülesannet sai lahendada, rakendades Eukleidese teoreemi mõttekäiku elemendile $a := 5(\prod_i p_i)^2 - 1$. Lisaks on vaja tähele panna, et iga a algteguri $p > 5$ (ilmselt $5 \nmid a$) korral on 5 ruutjääk, mis on võimalik vaid juhul $p \equiv \pm 1 \pmod 5$ (13. praktikumi 5. ülesanne). Aga kõik algtegurid ei saa olla kujul $5k+1$, sest siis nende korrutis a oleks ka kujul $5k+1$, aga ta on kujul $5k-1$. Seega leidub algtegur $p \mid a$, mis on kujul $5k-1$, järelikult võrdne ühega arvudest p_i. Siis aga $p \mid a - 5(\prod_i p_i)^2 = 1$, vastuolu.