Kevad 2015

Märkusi arvuteooria 6. praktikumi kohta:

A. Kommentaare ülesannete kaupa:

1. Selles ülesandes tuli lihtsalt leida

$$\varphi(2015) + \varphi(\frac{2015}{5}) + \varphi(\frac{2015}{13}).$$

Tüüpveaks oli siin see, et liidetavaid kas tekkis juurde juurde (näiteks $\varphi(\frac{2015}{10})$, mida ei ole vaja) või kadus ära (näiteks $\varphi(2015)$). Oma lahenduse optimeerimisel võib arvestada, et tegelikult ei ole tarvis leida $\frac{2015}{5} = 403$ täpset väärtust, vaid meile piisab algteguriteks lahutusest $\frac{2015}{5} = \frac{5 \cdot 13 \cdot 31}{5} = 13 \cdot 31$. Lisamärkusena, kui ülesandes oleks olnud 15 asemel suurima ühisteguri piiriks näiteks 150, siis oleks pidanud vaatama mitte ainult tegureid $1, 5, 13$ ja 31, vaid ka korrutist $5 \cdot 13$.

2. Üldiselt lahendati see ülesanne ära otse Euleri φ-funktsiooni standardkujust arvutamise valemi abil. See lähenemine on mõnevõrra töömahukas ja arvutusi saab tunduvalt vähendada, kui panna tähele, et kõik φ-funktsiooni argumendid selles ülesandes on arvu 60 jagajad. Puudu on vaid 1 ja 60, seega Gaussi teoreemi kohaselt $\varphi(1) + S + \varphi(60) = 60$ ja

$$S = 60 - \varphi(1) - \varphi(60) = 60 - 1 - 16 = 43.$$

3. Euleri funktsooni lahendamiseks rakendada üldiselt osati küll, aga mooduli järgi arvutamine võis siin alt vedada. Üks optimaalne arvutusvõimalus:

$$3^{2015} = 3^{8 \cdot 251 + 7} = (3^8)^{251} \cdot 3^7 \equiv 1 \cdot 27^2 \cdot 3 \equiv 11^2 \cdot 3 = 11 \cdot 33 \equiv 11 \pmod{16}.$$

Ja kuueteistkümnendsüsteemis on arvu 11 tähistav number tavaliselt B, mitte 11, või veel vähem 1.

4. See ülesanne osutus võrdlemisi keeruliseks, seega toon siinkohal ära täieliku lahenduse. Algteguriteks lahutades $133 = 7 \cdot 19$, seega järelduse 4.3 põhjal piisab, kui me tõestame, et

$$a^{145} \equiv a \pmod{7} \quad \text{ja} \quad a^{145} \equiv a \pmod{19}.$$

Kuna 7 on algarv, siis on meil kaks võimalust: kas $(a,7)=1$ või $7 \mid a$. Viimasel juhul $a \equiv 0 = 0^{145} \equiv a^{145} \pmod 7$. Kui aga $(a,7)=1$, siis Fermat' väikese teoreemi põhjal $a^6 \equiv 1 \pmod 7$, kust $a^{145} = (a^6)^{24} \cdot a \equiv 1^{24} \cdot a = a \pmod 7$. Seega tõepoolest alati $a^{145} \equiv a \pmod 7$. Tõestus arvu 19 jaoks on täiesti analoogiline, kuid kasutab fakti, et $a^{18} \equiv 1 \pmod{19}$, kust $a^{145} = (a^{18})^8 \cdot a \equiv 1^8 \cdot a = a \pmod{19}$.

5. Paljud kasutasid selle ülesande juures σ-funktsiooni nõrka aditiivsust (mõnikord ilma tõestuseta) ja selle väärtuste leidmist teguritel. Tegelikult sai siin koheselt rakendada teoreemi 5.21, sest $2^{n-1}(2^n-1)$ ongi juba antud standardkujul.

6. Muutus kahetärniülesandeks, sest selle lahendas ära vaid üks üliõpilane. Toon siinkohal ära tõestuse, mille visandasin praktikumis tahvlile. Esiteks, φ on nõrgalt aditiivne tänu teoreemile 5.7. Lisaks on ka μ nõrgalt aditiivne. Tõepoolest, kui $m,n \in \mathbb{N}$ on sellised, et $(m,n)=1$, siis on meil kolm võimalust:

a) kas $m=1$ või $n=1$ (üldisust kitsendamata olgu näiteks $n=1$), millisel juhul $\mu(mn)=\mu(m)=\mu(m)\cdot 1=\mu(m)\cdot\mu(1)=\mu(m)\cdot\mu(n)$,

b) leidub $p \in \mathbb{P}$ nii, et $p^2 \mid m$ või $p^2 \mid n$; olgu jälle üldisust kitsendamata $p^2 \mid n$, siis ka $p^2 \mid mn$ ja $\mu(mn)=0=\mu(m)\cdot 0=\mu(m)\cdot\mu(n)$,

c) $m=p_1\cdot\ldots\cdot p_s$ ja $n=q_1\cdot\ldots\cdot q_t$, kus $(m,n)=1$ tõttu peavad p_i ja q_i kõik olema erinevad algarvud, mistõttu mn esitub algteguriteks lahutatuna kui $mn=p_1\cdot\ldots\cdot p_s\cdot q_1\cdot\ldots\cdot q_t$; seega $\mu(mn)=(-1)^{s+t}=(-1)^s\cdot(-1)^t=\mu(m)\cdot\mu(n)$.

Tähistame $n=2^s\cdot n'$, kus $(2,n')=1$. Siis ka $(2^s,n')=1$. Nüüd paneme tähele, et $d \mid n$ parajasti siis, kui $d=e\cdot f$, kus $e \mid 2^s$ ja $f \mid n'$. Tõepoolest, tarvilikkuse jaoks teame juba, et $2^s=e\cdot e'$ ja $n'=f\cdot f'$, $e',f' \in \mathbb{Z}$, millest ilmselt

$$(e\cdot f)\cdot(e'\cdot f')=(e\cdot e')\cdot(f\cdot f')=2^s\cdot n'=n$$

ehk $e\cdot f \mid n$. Teisalt, kui $d \mid n$, siis võttes $e=(d,2^s)$ saame, et $d=e\cdot f$, kus $(f,2^s)=1$. Kuna $f \mid d$ ja $d \mid n=2^s\cdot n'$, siis $f \mid 2^s\cdot n'$. Eukleidese lemma tõttu $f \mid n'$ ja olemegi saanud, et $d=e\cdot f$, kus $e=(d,2^s) \mid 2^s$ ja $f \mid n'$. Seega võime kirjutada, et

$$\sum_{d\mid n}\varphi(d)\mu(d)=\sum_{e\mid 2^s}\sum_{f\mid n'}\varphi(ef)\mu(ef).$$

Pannes tähele, et eelneva tõestuse kohaselt $(e,f)=1$ (muidu $(f,2^s)>1$), saame nõrka multiplikatiivsust kasutades, et

$$\sum_{e|2^s}\sum_{f|n'}\varphi(ef)\mu(ef)=\sum_{e|2^s}\sum_{f|n'}\varphi(e)\mu(e)\varphi(f)\mu(f)$$
$$=\left(\sum_{e|2^s}\varphi(e)\mu(e)\right)\cdot\left(\sum_{f|n'}\varphi(f)\mu(f)\right).$$

Vaatleme selle korrutise esimest tegurit. Kuna $\mu(2^k)=0$ iga $k>1$ korral ja arvu 2^s tegurid on alati kujul 2^k, $k\geq 0$, siis

$$\sum_{e|2^s}\varphi(e)\mu(e)=\varphi(1)\mu(1)+\varphi(2)\mu(2)=1\cdot 1+1\cdot(-1)=0.$$

Järelikult on esimene tegur ja seetõttu ka terve summa alati võrdne nulliga.

7. Lahendusidee peale tuli enamus, aga selle põhjendamine jäi tihti üldsõnaliseks. Kusjuures õige vastuse korrektne kuju on: kas $n=p^9$, $p\in\mathbb{P}$, või $n=p\cdot q^4$, kus p ja q on erinevad algarvud. Standardkujust tuletatud lahendite puhul jäi tihti mulje, et alati kas $p<q$ või $p>q$ või isegi $n=p_1^{k_1}\cdot p_2^{k_2}\cdot p_3^9$.

8. Tegelikult kehtib antud ülesande väide ka algarvude 3 ja 7 korral. On lihtne näha, et iga $n\in\mathbb{N}$ ja $p\in\mathbb{P}$, $p>5$, korral annab Fermat' väike teoreem, et

$$10^{n(p-1)}=(10^{p-1})^n\equiv 1^n=1 \pmod{p}$$

ehk

$$10^{n(p-1)}-1=\underbrace{99\ldots9}_{n(p-1)}\equiv 0 \pmod{p}.$$

Kui $p\neq 3$, siis $(p,9)=1$ ja

$$\frac{10^{n(p-1)}-1}{9}=\underbrace{11\ldots1}_{n(p-1)}\equiv 0 \pmod{p}$$

ehk $p\mid\underbrace{11\ldots1}_{n(p-1)}$. Kui $p=3$, siis $p\mid\underbrace{111}_{3n}$. Seega on meil iga naturaalarvu n jaoks järjest kasvavad p kordsed jada liikmed $\underbrace{11\ldots1}_{n(p-1)}$ (või $\underbrace{11\ldots1}_{3n}$), milliseid ongi kokku lõpmata palju.