Mat-tanári gyakorlat, első évfolyam, második félév
Hetedik alkalom

1. *Oldjuk meg a $\varphi(x) = x - 2$ illetve a $\varphi(x) = 6$ egyenletet.*

2. *Mutassuk meg a képlet felhasználása nélkül, hogy $n > 2$ esetén $\varphi(n)$ páros szám. Mutassuk meg, hogy van végtelen sok olyan páros szám, ami nincs benne φ értékkészletében.*

3. *Határozzuk meg 97^{227} és 97^{223} maradékát 113-mal osztva.*

4. *Bizonyítsuk be, hogy 1997-nek végtelen sok olyan többszöröse van, amely a tizes számrendszerben csupa 9-es számjegyből áll. Milyen számokra igaz még ez? (HF*: igazoljuk, hogy minden racionális szám (végtelen) tizedestört alakja periódikus.)*

5. *Fejtsük meg az $n = 91$ és $s = 41$ nyilvános kódú személy titkos kulcsát, és dekódoljuk a neki küldött (egy blokkból álló) 29 üzenetet. Törjük fel az $n = 7081$, $s = 2765$ kódot is.*

6. *Mely m-ekre igaz, hogy minden a és k esetén $k \equiv 1\ (\varphi(m)) \implies a^k \equiv a\ (m)$?*

7. *Azt mondjuk, hogy az $n > 1$ összetett szám abszolút álprím, ha minden n-hez relatív prím $a > 1$ egészre $a^{n-1} \equiv 1\ (n)$. Ha ezt a tulajdonságot csak $a = 2$-re követeljük meg, akkor az álprímeket kapjuk. Igazoljuk az alábbi állításokat.*
a) Ha $\varphi(n) \mid n - 1$, akkor n abszolút álprím.
b) Az $n = 561 = 3 \cdot 11 \cdot 17$ szám abszolút álprím.
c) A $341 = 11 \cdot 31$ szám álprím, de nem abszolút álprím ($a = 3$ lebuktatja).
d) Ha n álprím, akkor $2^n - 1$ is az.
e) Legyen $F_n = 2^{2^n} + 1$. Ekkor $F_{100}F_{200}F_{300}$ álprím.

Gyakorló feladatok

8. *Igaz marad-e $\varphi(n)$ képlete, ha n kanonikus alakjában nulla kitevőket is megengedünk?*

9. *Mi a nagyságviszony $\varphi(mn)$ és $\varphi(m)\varphi(n)$ között? Mikor áll egyenlőség?*

10. *Mutassuk meg, hogy ha m és n relatív prímek, akkor egy m-edik és egy n-edik primitív egységgyök szorzata mindig mn-edik primitív egységgyök (vö. előző félév X/5/c), továbbá, hogy minden mn-edik primitív egységgyök előáll egy m-edik és egy n-edik primitív egységgyök szorzataként. Vezessük le ebből, hogy az Euler-függvény multiplikatív.*

11. *Definiáljuk a $\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ halmazon a szorzást így: $(a, b)(c, d) = (a \cdot_m c, b \cdot_n d)$. Mutassuk meg, hogy csoportot kaptunk, és ha $(m, n) = 1$, akkor az előadáson az Euler-függvény multiplikatívitásának bizonyításában megadott $\Psi : \mathbb{Z}_{mn}^\times \to \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ leképezés művelettartó.*

12. *Oldjuk meg az alábbi egyenleteket.*
a) $\varphi(x) = x - 3$.
b) $\varphi(2x) = 2\varphi(x)$.
c) $\varphi(3x) = \varphi(5x)$.
d) $\varphi(x) = x/2$.
e) $\varphi(x) + d(x) = x + 1$.

13. *Mutassuk meg, hogy $m \mid n \implies \varphi(m) \mid \varphi(n)$. Milyen n-ekre teljesül, hogy $\varphi(n) \mid n$?*

14. *Keressünk a nyilvános kulcsú titkosírás alapján olyan módszert, amellyel a küldő hamisíthatatlanul és letagadhatatlanul aláírhatja a levelét (pl. rendelkezhessen a számlájáról).*