Bevezetés a Számításelméletbe I. — *emelt szintű* kurzus
Negyedik gyakorlat, 2023. október 3.

1. A $C : x \mapsto x^{43} \pmod{91}$ kódoló függvénnyel a $0, 1, \ldots 90$ „üzeneteket" lehet kódolni. Határozzuk meg a C-hez tartozó D dekódoló függvényt.

---

2. Hány olyan 504-nél nem nagyobb, pozitív egész szám van, amelynek van 504-gyel osztva 1 maradékot adó többszöröse? (ZH, 2019. december 16.)

3. Legyen n egy 8-cal osztható, de 3-mal nem osztható pozitív egész szám. Mutassuk meg, hogy a 3 árulója n-nek (vagyis a Fermat-teszt végrehajtásakor a 3 tanúsítja n összetett voltát). (ZH, 2018. október 18.)

4. Határozzuk meg az összes olyan 1 és 100 közti a egész számot, melyre $a^{21} \equiv 1 \pmod{100}$. (ZH, 2020. december 14.)

5. Létezik-e páros Carmichael-szám? (ZH, 2017. október 19.)

6. Milyen maradékot ad $100^{3^{2011}}$ 3^{2011}-nel osztva? (ZH, 2011. április 21.)

---

7. Legyen $n = 987654321$. Az előadáson tanult megfelelő algoritmus alkalmazásával határozzuk meg $98n + 27$ és $76n + 21$ legnagyobb közös osztóját. (ZH, 2020. december 21.)

8. – Mi legyen ebédre?
– Hát, mondjuk...
– Vigyázz, az ellenség lehallgatja a beszélgetést! Használd a $C : x \mapsto x^{11} \pmod{51}$ kódoló függvényt úgy, hogy az angol ábécé betűit sorban a 1, 2, ..., 26 számokkal helyettesíted!
– Mármint...
– Ne értetlenkedj! $A = 1$, $B = 2$, $C = 3$, satöbbi, végül $Z = 26$. Ékezeteket ne használj és ne törődj azzal, hogy 50-ig a többi számnak már nincs jelentése. Szóval mi legyen a kaja?
– 2, 1, 6.
Készítsünk dekódoló függvényt és fejtsük meg vele, hogy mi lesz az ebéd.

9. Döntsük el az alábbi számokról, hogy 165-nek árulója, cinkosa vagy egyik sem. (A megoldáshoz használjunk számológépet és a megfelelő, tanult algoritmusokat.)

a) 13 b) 23 c) 33

10. Bizonyítsuk be, hogy 561 ($= 3 \cdot 11 \cdot 17$) Carmichael-szám.

11. Bizonyítsuk be, hogy ha a egy 11-gyel nem osztható egész szám, akkor az $x^3 \equiv a \pmod{121}$ kongruencia megoldható (vagyis létezik olyan x egész, amelyre a kongruencia fennáll). (ZH, 2009. április 24.)

12. Definiáljuk a $\gamma(m)$ függvényt: $\gamma(m) = [p_1^{\alpha_1} - p_1^{\alpha_1 - 1}, p_2^{\alpha_2} - p_2^{\alpha_2 - 1}, \ldots, p_k^{\alpha_k} - p_k^{\alpha_k - 1}]$, ahol az $m > 1$ egész prímtényezős felbontása $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ (és a [ ] a legkisebb közös többszöröst jelöli). Bizonyítsuk be az Euler-Fermat tétel következő élesítését: ha $(a, m) = 1$, akkor $a^{\gamma(m)} \equiv 1 \pmod{m}$.

13. Legyen $a_1, \ldots, a_{\varphi(m)}$ az m-nél kisebb, m-hez relatív prím pozitív egészek halmaza. Hasonlóan, legyen $b_1, \ldots, b_{\varphi(n)}$ az n-nél kisebb, n-hez relatív prím számok halmaza.

a) Mutassuk meg, hogy ha m és n relatív prímek, akkor minden $1 \le i \le \varphi(m)$ és $1 \le j \le \varphi(n)$ esetén pontosan egy olyan mn-nél kisebb x szám van, amelyre $x \equiv a_i \pmod{m}$ és $x \equiv b_j \pmod{n}$.

b) Mutassuk meg, hogy az így kapott x relatív prím mn-hez.

c) Bizonyítsuk be a fentieket használva, hogy ha m és n relatív prímek, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

14. Mutassuk meg, hogy $n \mid \varphi(k^n - 1)$ igaz minden $k, n \ge 1$ egészekre.

15. Bizonyítsuk be, hogy ha egy p prím osztója $2^{2^n} + 1$-nek, akkor $p \equiv 1 \pmod{2^{n+1}}$.

16. Egy n egész minden d pozitív osztójára kiszámoljuk $\varphi(d)$ értékét és a kapott számokat összeadjuk. Mit kapunk?

17*. Minden m pozitív egészre határozzuk meg az m-nél kisebb, m-hez relatív prím pozitív egészek szorzatának m szerinti osztási maradékát.