SzA XII. gyakorlat

$P?NP$, továbbá 3+2 néha = 1

2010. november 24/25.

Hasznos tudnivalók

- **NP-teljesség bizonyítása** L problémára:
  1. L NP-beliségének bizonyítása.
  2. L NP-nehézségének bizonyítása:
     (a) Találunk egy vele kapcsolatba hozható problémát, ami ismerten NP-teljes, ez legyen I.
     (b) Bemutatunk egy $I \prec L$ Karp-redukciót, az irány fontos!
     (c) Bizonyítjuk a Karp-redukció helyességét. Azaz, ha f az átalakítás: $x \in I \Leftrightarrow f(x) \in L$ a bizonyítandó. Figyelem! Akkor és csak akkor!
     (d) Belátjuk, hogy f polinom időben elvégezhető.

- Ha $a \equiv b \pmod{m}$, akkor
  - $a \pm c \equiv b \pm c \pmod{m}$ $\qquad$ $a \cdot c \equiv b \cdot c \pmod{m}$
  - $\frac{a}{c} \equiv \frac{b}{c} \pmod{\frac{m}{c}}$, ha $c \mid a, b, m$ $\qquad$ $\frac{a}{c} \equiv \frac{b}{c} \pmod{m}$, ha $(c, m) = 1$
  - $a \cdot c \equiv b \cdot d \pmod{m}$, ha $c \equiv d \pmod{m}$

- $a \cdot x \equiv b \pmod{m}$ lineáris kongruenciának
  - $\exists$ megoldása $\Leftrightarrow (a, m) \mid b$
  - $\exists$ megoldása $\Leftrightarrow (a, m) \pmod{m}$ megoldása létezik

- Euler-Fermat témakör
  - $\varphi(m)$: 1 és m közötti m-hez relatív prímek száma; $\varphi(p) = p - 1$, ha p prím
  - $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, ha p prím
  - $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, ha $(a, b) = 1$
  - Ha $(a, m) = 1$, akkor $1 \equiv a^{\varphi(m)} \pmod{m}$
  - Ha p prím és $p \nmid a$, akkor $a^{p-1} \equiv 1 \pmod{p}$
  - Ha p prím, akkor $a \equiv a^p \pmod{p}$

- Wilson-tétel

$$(n-1)! \equiv \begin{cases} -1 \pmod{n} & \text{ha } n \text{ prím} \\ 2 \pmod{n} & \text{ha } n = 4 \\ 0 \pmod{n} & \text{ha } n > 4 \text{ összetett} \end{cases}$$

---

1. A G irányítatlan gráf minden x pontjához tartozik egy $s(x)$ súly. Célunk, hogy olyan feszítőfát találjunk a gráfban, amiben a levelekhez tartozó súlyok összege minimális. Adjuk meg a feladathoz tartozó L nyelvet, majd adjunk Karp-redukciót a H-út nyelvről L-re!

2. **[ZH 2008. november 17.]** Bizonyítsuk be, hogy NP-teljes az a π döntési probléma, aminek a bemenete egy $100n$ pontú irányítatlan gráf, a kimenete pedig pontosan akkor „*igen*", ha G-nek van legalább n pontú köre.

3. **[PZH 2008. december 5.]** Bizonyítsuk be, hogy NP-teljes az a π döntési probléma, aminek a bemenete egy egyszerű G gráf, az n és m számok, a kimenete pedig pontosan akkor „*igen*", ha G-nek van olyan n csúcsú részgráfja, aminek legalább m éle van.

4. Határozzuk meg az Euklidészi algoritmussal $lnko(504, 372)$-t! Határozzuk meg $lkkt(504, 372)$-t! Hány osztója van 504-nek?

5. Van-e olyan a és b szám, hogy $lnko(a, b) = 3$ és $a+b = 100$? És ha $lnko(a, b) = 5$?

6. Bizonyítsuk be, hogy a $\frac{21n+4}{14n+3}$ tört semmilyen n-re nem egyszerűsíthető!

7. Bizonyítsuk be, hogy ha az $n > 1$ számnak 2005 osztója van, akkor n nem lehet egy egész szám ötödik hatványa!

8. **[ZH 2008. november 17.]** Igazoljuk, hogy ha m és n pozitív egészek, akkor $d(n)d(m) = d(lnko(n, m))d(lkkt(n, m))$ teljesül, ahol $d(k)$ a k pozitív osztóinak számát, $lnko(n, m)$ és $lkkt(n, m)$ pedig rendre az n és m legnagyobb közös osztóját ill. legkisebb közös többszörösét jelölik.

9. **[PZH 2008. december 5.]** Tudjuk, hogy n és m olyan pozitív egészek, amikre $lnko(n, m) = 10$ és $lkkt(n, m) = 1000$, ahol $lnko(n, m)$ és $lkkt(n, m)$ pedig rendre az n és m legnagyobb közös osztóját ill. legkisebb közös többszörösét jelölik. Határozzuk meg az nm szorzatot.

10. A $\{0, 1, \ldots, 16\}$ mod 15 teljes maradékrendszer mely elemeihez tartoznak a következő számok: 221, 152, 193, 46, 66, 209, 11980, 46628?

11. Bizonyítsuk be, hogy minden n természetes számra $n^7 - n$ osztható 42-vel!

12. Bizonyítsuk be, hogy $39^{14} - 1$ osztható 5-tel!

13. Gyorshatványozással számítsuk ki $7^{19} \pmod 5$ értékét!

14. Mi az alábbi lineáris kongruenciák megoldása?

    (a) $9x \equiv 24 \pmod{96}$
    (b) $8x \equiv 3 \pmod{21}$

15. Határozzuk meg x-et!

    (a) $5^{1997} \equiv x \pmod{17}$
    (b) $108^{182} \equiv x \pmod{19}$
    (c) $49^{49} \equiv x \pmod{15}$
    (d) $42^{600} \equiv x \pmod{13}$
    (e) $205^{206^{207}} \equiv x \pmod{103}$
    (f) $x^{11999} \equiv 5 \pmod{13}$
    (g) $1998! + 111^{1998} \equiv x \pmod{1999}$

16. Bizonyítsuk be, hogy tetszőleges p prímszámra: $(a + b)^p \equiv a^p + b^p \pmod p$