

SzA XII. gyakorlat

$P \stackrel{?}{=} NP$, továbbá $3+2$ néha $= 1$

2010. november 24/25.

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!

A nyelv (azaz az eldöntési probléma):

$$L = \left\{ (G, k) \mid \begin{array}{l} G \text{ irányítatlan csúcssúlyozott gráf, amiben van} \\ \text{legfeljebb } k \text{ levélsúlyú feszítőfa} \end{array} \right\}$$

Ez NP -teljes. NP -beli, mert egy jó tanú egy ilyen feszítőfa (ellenőrzés polinom időben megy, a mérete is polinom). Adunk egy H -út $\prec L$ Karp-redukciót. Ha egy G gráfban Hamilton-utat keresünk, akkor minden csúcshoz rendeljünk 1 súlyt, és az így keletkezett G' gráfban keressünk legfeljebb 2 levélsúlyú feszítőfát! Állítás: $G \in H\text{-út} \Leftrightarrow (G', 2) \in L$. $G \in H\text{-út} \Rightarrow (G', 2) \in L$: G egy Hamilton-útja pont egy két levelű, 2 súlyú feszítőfa G' -ben. $(G', 2) \in L \Rightarrow G \in H\text{-út}$: egy ilyen feszítőfának pontosan 2 levele kell, hogy legyen (ha több lenne, nagyobb lenne a súlya, egy fában pedig mindig van legalább 2 levél). Ez pedig pont egy olyan utat jelent, ami tartalmazza a gráf összes csúcsát, tehát G egy Hamilton-útját. A csúcsoknak súlyt adni lehet polinom időben.

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.

NP -beli: Tanú egy ilyen kör, ellenőrizni kell, hogy a gráf tényleg $100n$ pontú-e, és a kör tényleg kör-e és n pontú-e. A tanú mérete n ami $100n$ polinomja, az ellenőrzés legfeljebb n lépés után véget ér, tehát ez is polinomiális.

NP -nehéz, mert $H\text{-kör} \prec \pi$. Adott G gráfhoz vegyünk hozzá $99n$ pontot, ez G' . Van $H\text{-kör}$ G -ben $\Leftrightarrow$ van n pontú kör G' -ben. Van $H\text{-kör}$ G -ben $\Rightarrow$ van n pontú kör G' -ben: tñh van $H\text{-kör}$ G -ben, akkor ez pont egy n pontú kör G' -ben, ami $100n$ csúcsú, vagyis a feltétel teljesül. Van $H\text{-kör}$ G -ben $\Leftarrow$ van n pontú kör G' -ben: az izolált pontokon nyilván nem mehet át a kör, tehát csak az eredeti gráfban mehet, de G -ben egy n hosszú kör pont $H\text{-kör}$. $99n$ pont felvétele polinom idő, tehát az átalakítás polinomiális.

A probléma NP -beli és NP -nehéz, tehát NP -teljes.

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.

NP -beli: tanú egy ilyen részgráf, mérete nem lehet nagyobb a gráfénál, tehát polinomiális, az ellenőrzés pedig azt jelenti, hogy megnézzük, hogy tényleg részgráf-e, valamint a csúcsok és élek száma rendben van-e, ez nyilván polinomiális.

NP -nehéz, mert $MAXKLIKK \prec \pi$. Ha G -ben valaki megkérdezi, hogy van-e k pontú klikk, akkor kérdezzük meg G -ről, hogy van-e benne k pontú és $\binom{k}{2}$ élű

részgráf. G -ben van k pontú klikk $\Leftrightarrow G$ -ben van k pontú és $\binom{k}{2}$ élű részgráf. G -ben van k pontú klikk $\Rightarrow G$ -ben van k pontú és $\binom{k}{2}$ élű részgráf: G egy k pontú klikkje pont megfelelő. G -ben van k pontú klikk $\Leftarrow G$ -ben van k pontú és $\binom{k}{2}$ élű részgráf: ez a részgráf G egyszerűsége miatt nyilván csak a K_k lehet, ami def szerint egy k pontú klikk G -ben. Az átalakításhoz csak $\binom{k}{2}$ -t kell kiszámolni, ami nyilván polinom idő.

A probléma NP -beli és NP -nehéz, tehát NP -teljes.

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

$$504 = 1 \cdot 372 + 132$$

$$372 = 2 \cdot 132 + 108$$

$$132 = 1 \cdot 108 + 24$$

$$108 = 4 \cdot 24 + 12$$

$$24 = 2 \cdot 12 + 0,$$

tehát $lnko(504, 372) = 12$.

$lnko(x, y) \cdot lkkt(x, y) = x \cdot y$, ezért $lkkt(504, 372) = 504 \cdot 372 / 12 = 15624$. Másképp is lehet, a prímfelbontások alapján $504 = 2^3 \cdot 3^2 \cdot 7$, $372 = 2^2 \cdot 3 \cdot 31$, ezért $lkkt(504, 372) = 2^3 \cdot 3^2 \cdot 7 \cdot 31 = 15624$.

$504 = 2^3 \cdot 3^2 \cdot 7$, ezért $(3 + 1)(2 + 1)(1 + 1) = 24$ osztója van.

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

Az első esetben 3 osztója mindkét számnak, azaz $a = 3k$ és $b = 3l$, ekkor $a + b = 3(k + l) = 100$, 100 viszont nem osztható hárommal, tehát nincs. A második esetben igen, pl. 55 és 45.

6. **Bizonyítsuk be, hogy a $\frac{21n+4}{14n+3}$ tört semmilyen n -re nem egyszerűsíthető! Keressük meg $lnko$ -t! Euklidészi algoritmussal:**

$$21n + 4 = 1 \cdot (14n + 3) + (7n + 1)$$

$$14n + 3 = 2 \cdot (7n + 1) + 1$$

$$7n + 1 = 1 \cdot (7n + 1) + 0,$$

vagysis a számláló és nevező relatív prím.

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

Ha n egy egész szám ötödik hatványa, akkor a prímtényezős felírásban a kitevők így néznek ki: $5\alpha_1, \dots, 5\alpha_k$, tehát osztóinak száma $(5\alpha_1 + 1) \dots (5\alpha_k + 1)$. 2005 prímtényezős felbontása $5 \cdot 401$, viszont az osztók száma nem osztható 5-tel (minden tag $5\alpha_i + 1$ alakú).

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.**

Fel fogjuk használni, hogy $\min(a, b) \max(a, b) = ab$, valamint $\min(a, b) + \max(a, b) = a + b$. n és m kanonikus alakjával fogunk dolgozni, $n = \prod_{i=1}^k p_i^{\alpha_i}$

és $m = \prod_{i=1}^k p_i^{\beta_i}$.

Bal oldal: $d(n)d(m) = \prod_{i=1}^k (\alpha_i + 1)(\beta_i + 1) = \prod_{i=1}^k (\alpha_i \beta_i + \alpha_i + \beta_i + 1)$

Jobb oldal: $d(\lnko(n, m))d(\lkkt(n, m)) = \prod_{i=1}^k (\min(\alpha_i, \beta_i) + 1)(\max(\alpha_i, \beta_i) + 1) = \prod_{i=1}^k (\min(\alpha_i, \beta_i) \max(\alpha_i, \beta_i) + \min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) + 1) = \prod_{i=1}^k (\alpha_i \beta_i + \alpha_i + \beta_i + 1)$.

Azaz ekvivalens átalakításokkal ugyanarra jutottunk, tehát az állítás igaz.

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.

Tétel: $\lnko(n, m)\lkkt(n, m) = nm$. Ebből $nm = 10 \cdot 1000 = 10000$.

10. A $\{0, 1, \dots, 16\} \pmod{17}$ teljes maradékrendszer mely elemeihez tartoznak a következő számok: 221, 152, 193, 46, 66, 209, 11980, 46628?

0, 16, 6, 12, 15, 5, 12, 14, ha nem gépeltem vagy számoltam el valamit.

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

Azt kell belátni, hogy $n^7 - n$ osztható 2-vel, 3-mal és 7-tel. $n^7 - n = n(n^6 - 1) = n(n^3 - 1)(n^3 + 1)$. 2-vel oszthatóság triviális (n^7 és n paritása azonos, így különbségük páros). Héttel oszthatóság ekvivalens azzal, hogy $(\pmod{7}) 0$ az eredmény, kis-Fermat tétel alapján $n^7 - n \equiv n - n \equiv 0 \pmod{7}$. 3-mal oszthatóság: $n(n^3 - 1)(n^3 + 1) \equiv n(n - 1)(n + 1)$ kis-Fermat tétel alapján, azaz három egymást követő szám szorzata, amiből az egyik biztos osztható 3-mal.

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

$39^{14} - 1 \equiv (-1)^{14} - 1 \equiv 1 - 1 \equiv 0 \pmod{5}$.

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

$19 = 10011_b = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$.

7 hatványai: $7^{2^0} \equiv 2 \pmod{5}$, $7^{2^1} \equiv 7^{2^0} \cdot 7^{2^0} \equiv 4 \pmod{5}$, $7^{2^2} \equiv 7^{2^1} \cdot 7^{2^1} \equiv 1 \pmod{5}$, $7^{2^3} \equiv 7^{2^2} \cdot 7^{2^2} \equiv 1 \pmod{5}$, $7^{2^4} \equiv 7^{2^3} \cdot 7^{2^3} \equiv 1 \pmod{5}$.

Így $7^{19} \equiv 1 \cdot 2 \cdot 4 \equiv 3 \pmod{5}$.

14. Mi az alábbi lineáris kongruenciák megoldása?

(a) $9x \equiv 24 \pmod{96}$

$(9, 96) = 3$, és $3 \mid 24$, tehát van megoldás, és 3 megoldás van.

$$3x \equiv 8 \pmod{32}$$

$$3x \equiv 72 \pmod{32}$$

$$x \equiv 24 \pmod{32}$$

A 3 megoldás tehát:

$$x_1 \equiv 24 \pmod{96}$$

$$x_2 \equiv 56 \pmod{96}$$

$$x_3 \equiv 88 \pmod{96}$$

(b) $8x \equiv 3 \pmod{21}$

$(8, 21) = 1$, és $1 \mid 3$, tehát van megoldás, és 1 megoldás van.

$$8x \equiv 3 \pmod{21}$$

$$8x \equiv 24 \pmod{21}$$

$$x \equiv 3 \pmod{21}$$

15. Határozzuk meg x -et!

(a) $5^{1997} \equiv x \pmod{17}$

$(5, 17) = 1$, tehát az Euler-Fermat tétel használatával:

$$5^3 \cdot 5^{1997} \equiv 5^3 \cdot x \pmod{17}$$

$$5^{2000} \equiv 6x \pmod{17}$$

$$(5^{16})^{125} \equiv 6x \pmod{17}$$

$$1^{125} \equiv 6x \pmod{17}$$

$$6x \equiv 1 \pmod{17}$$

$$6x \equiv 18 \pmod{17}$$

$$x \equiv 3 \pmod{17}$$

(b) $108^{182} \equiv x \pmod{19}$

(c) $49^{49} \equiv x \pmod{15}$

(d) $42^{600} \equiv x \pmod{13}$

(e) $205^{206^{207}} \equiv x \pmod{103}$

$$205^{206^{207}} \equiv (-1)^{206^{207}} \equiv 1 \equiv x \pmod{103}$$

(f) $x^{11999} \equiv 5 \pmod{13}$

$(x, 13) = 1$, különben a bal oldal 0 lenne. Euler-Fermat használatával:

$$x^{12000} \equiv 5x \pmod{13}$$

$$(x^{12})^{1000} \equiv 5x \pmod{13}$$

$$1 \equiv 5x \pmod{13}$$

$$5x \equiv 1 \pmod{13}$$

$$5x \equiv 40 \pmod{13}$$

$$x \equiv 8 \pmod{13}$$

(g) $1998! + 111^{1998} \equiv x \pmod{1999}$

Wilson-tétel és Euler-Fermat tétel használatával (a feltételek teljesülnek, 1999 prím): $1998! + 111^{1998} \equiv -1 + 1 \equiv 0 \equiv x \pmod{1999}$.

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

Kis-Fermat tétel használatával triviális.