Bevezetés a Számításelméletbe 2.

Konzultáció
(Összefoglalás)
2009. 10. 21.

A ZH feladatok megoldása előtt mindenki próbálja besorolni, hogy egy-egy feladat milyen témakörhöz kapcsolódik. A nagy valószínűséggel előforduló témakörök a következők: *Euler-körök, Hamilton-körök, Perfektség, Pontszínezés, Párosítás páros gráfon, Folyam.* Ez hat témakör a hat feladatra, általában minden feladat valamelyik témakörre rá is kérdez. Lehet még esetleg *élszínezés, párosítás tetszőleges gráfban, görög betűs feladat.*

1. *Euler-körök.* Erre tipikusan kétféleképp szoktak a ZHn rákérdezni. 1) „Le lehet-e rajzolni a ceruza felemelése nélkül az alábbi gráfot?" típusú kérdés, ahol ellenőrizni kell, vajon minden pont foka páros-e (és ekkor van Euler-kör, tehát igen), vagy ez nem így van, és akkor nem lehet. 2) Szöveges feladat, amiben minden, vagy „majdnem minden" pont foka páros. Ezeket addig kell gyúrni, amíg Euler-kört nem kap az ember. Soha ne feledkezzünk meg az összefüggőség ellenőrzéséről sem!

2. *Hamilton-körök.* A Hamilton-kör létezésére nincs szükséges és elégséges feltétel, de azért a ZHn többféleképpen lehet az ilyen feladatokat lekaszálni. Egyrészt néhány pontú gráfon az ember kézzel kereshet Hamilton-kört, ha talált nyert. Ha nem ilyen egyszerű a gráf, akkor reménykedhetünk abban, hogy a fokszámok nagyok, $d(x) \geq n/2$ minden, vagy „majdnem minden" csúcsra, és ekkor a Dirac-tétellel vagy az Ore-tétellel igazolhatjuk, hogy van Hamilton-kör. Ha ezek egyike sem segít, akkor nem marad más, mint az az eset, hogy nincs Hamilton-kör a gráfban, amit úgy látunk be, hogy k pontot elhagyunk, és a gráf legalább $k+1$ részre esik szét.

3. *Perfektség.* Talán ez a legkevésbé elképzelhető fogalom. Egy perfektes feladatot kétféle képpen lehet támadni aszerint, hogy a gráf perfekt, vagy sem (van, hogy a feladat előre megmondja, mit is kéne belátni „mutassuk meg, hogy az így nyert gráf perfekt..."). 1) Ha azt gondoljuk, hogy a gráf perfekt, akkor azt legegyszerűbben úgy lehet igazolni, hogy belátjuk, a gráf páros. Szinte lehetetlen azt belátni, hogy a gráfban sehol nincs legalább 5 hosszú, páratlan, húrnélküli kör (vagy annak komplementere), és aztán az erős perfekt gráf tételre hivatkozni. Ha mázlink van, a gráfot fel tudjuk rajzolni intervallumgráfként, és akkor automatikusan perfekt lesz. Ez elég macerás. 2) Ha a gráf nem perfekt, akkor azt úgy tudjuk igazolni, hogy egyetlen legalább 5 hosszú, páratlan, húr nélküli kört mutatunk benne (esetleg a gráf komplementerében), majd az erős perfekt gráf tételre hivatkozunk.

4. *Pontszínezés.* A pontszínezésnél két dologra kell figyelni: Egyrészt mutatni kell egy jó színezést k színnel, amiből következik, hogy $\chi(G) \leq k$, másrészt be kell látni, hogy ennél kevesebb szín nem elegendő. Ezt ZH-szinten úgy lehet igazolni, hogy egy k méretű klikket is mutat az ember, és innen $k \leq \omega(G) \leq \chi(G) \leq k$ egyenlőtlenség miatt valóban k a kromatikus szám. Ezt néha könnyebb fordítva csinálni, vagyis keresni egy jó nagy k-klikket, és a már felhasznált k szín segítségével megszínezni a többi csúcsot is. Érdemes a Brooks-tételt és a mohó színezést észben tartani.

5. *Párosítás páros gráfon.* Tipikus példa: adott egy 12 pontú, osztályonként 6-6 csúcsból álló páros gráf, élek össze-vissza a két osztály között. A kérdés van-e benne teljes párosítás. Ha van ilyen, azt a magyar módszerrel megtaláljuk, ha nincs, akkor azt a magyar módszerrel nem fogjuk megtalálni, viszont a bizonyíték, hogy nem mi vagyunk ügyetlenek, hanem tényleg nincs az az, hogy rámutatunk: sérül a Hall-feltétel, vagyis van olyan X halmaz, akinek a túloldalon túl kevés szomszéda van, tehát tényleg nem lehet teljes párosítást csinálni. Párosításos feladat lehet még valami elképzelhetetlen szöveges feladat, amit viszont k-reguláris páros gráfra lehet átvinni. A gyakorlaton megbeszéltük, hogy minden k-reguláris páros gráf felbomlik k éldiszjunkt teljes párosításra, és ebből általában kijön a feladat.

6. *Folyam.* A folyam biztos tíz pont. Folyamkeresés algoritmikusan, először csak előre éleken, ha ezeken már nincs javítóút, akkor a visszaélek behúzásával. Ha a visszaélekkel sem tudunk már javítani, akkor a talált folyam maximális. A bizonyíték (vö: páros gráfokban párosítás) arról, hogy tényleg nincs ennél nagyobb értékű folyam az az, hogy az ember egy, a talált folyam értékével megegyező vágást is mutat, amit a következőképpen keresünk meg. A legutolsó segédgráfban (amelyben már

visszaélek segítségével sincs javítóút) megnézzük, hogy S-ből kiket lehet elérni az előre illetve a visszaélek segítségével. Legyenek ezek a pontok az A halmazban, tehát $A := \{x \in V(G) : \text{Létezik } S \to x \text{ irányított út}\}$. A B halmaz mindenki, akit S-ből nem lehet elérni, vagyis $B := V(G) \setminus A$. A vágást azon élek alkotják, amelyek valamely A-beli pontból indulnak ki, és valamely B-belibe érkezenek érkeznek. Egy vágás nem biztos, hogy tényleg két komponensre vágja szét a gráfot, előfordulhat, hogy valamely B-ből A-ba mutató él „összetartja" a gráfot a vágás után is. De ilyen élek mentén már nem folyhat folyam. A Ford-Fulkerson tételre való hivatkozás ennél a feladatnál elengedhetetlen.

7. *Élszínezés.* Macerás. A Vizing-tétel miatt $\Delta \leq \chi_e \leq \Delta + 1$ teljesül. Ha a gráf $2k+1$, tehát páratlan pontú, és Δ-reguláris, akkor mindig $\Delta + 1$ szín kell a jó élszínezéshez. Bizonyítás: színosztályonként legfeljebb k él lehet (mivel minden él két csúcsot „letilt"), így Δ színosztállyal számolva összesen legfeljebb $\Delta \cdot k$ élet színeztünk meg. Na de összesen $e = \frac{1}{2} \cdot \sum d(x) = \frac{1}{2}\Delta(2k+1) = \Delta \cdot k + \frac{1}{2}\Delta$ élünk van. Vagyis egy hajszállal több. Ez az ellentmondás biztosítja, hogy $\Delta + 1$ szín kell az élszínezéshez.

8. *Párosítás tetszőleges gráfban.* Nem szokott ilyen feladat lenni. Ha mégis, akkor két esély van: 1) Hamilton-kör is van a gráfban (mondjuk nagyok a fokszámok, és Dirac), és akkor a Hamilton-kör minden második éle egy teljes párosítást alkot. 2) Egyszerű, néhány pontos példából k pontot elhagyva a gráf páratlan csúcsszámú komponensei száma legalább $k + 1$ lesz, akkor a Tutte-tétel miatt nincs teljes párosítás.

9. *Görög betűk.* Tipikus példa: adott egy néhány pontú gráf, határozzuk meg rá az $\alpha, \nu, \tau, \varrho$ értékeket. Ha nincs hurokél, és izolált pont (nem szokott lenni) akkor $\alpha + \tau = \nu + \varrho = n$. Tehát elég legfeljebb kettő betűt kitalálni. Páros gráfban (ha nincs izolált pont) akkor $\alpha = \varrho$ illetve $\nu = \tau$ is teljesül, tehát elég egyetlen betűt meghatározni. Vegyük észre, hogy ν a maximális független élek száma, vagyis a legnagyobb elemszámú párosítás páros gráf esetén a magyar-módszerrel, illetve a Hall-feltétellel támadható. Ha ν megvan, akkor a többi érték automatikusan adódik. Mindenképp figyeljünk arra, hogy ne csak azt mutassuk meg, hogy (pl.) $\alpha \geq k$, mert ennyi független pontot találunk, hanem mindenképpen érveljünk, hogy $\alpha \leq k$, vagyis hogy ennél többet meg nem is lehet találni.

Bevezetés a Számításelméletbe 2.

Konzultáció – Összefoglalás

2009. 11. 11.

A ZH feladatok megoldása előtt mindenki próbálja besorolni, hogy egy-egy feladat milyen témakörhöz kapcsolódik. A nagy valószínűséggel előforduló témakörök a következők: *Gráfok összefüggősége, Lineáris kongruenciák, Számelméleti függvények, Az Euler-Fermat tétel, Csoportaxiómák ellenőrzése, Absztrakt algebrai feladat.*

1. *Gráfok összefüggősége.* Ehhez a témakörhöz a két idevágó Menger-tételt kell tudni, vagyis azokat amelyek a pont- illetve az élösszefüggőséget karakterizálják. Ha véletlenül kört kell keresni a gráfban, akkor a második Dirac-tételt kell használni.

2. *Lineáris kongruenciák.* Ha van egy $ax \equiv b \pmod{(m)}$ kongruenciánk, akkor az első kérdés ez: Megoldható a kongruencia? Erre a válasz: igen, pontosan akkor, ha $(a,m)|b$. A második kérdés: Hány megoldást kapunk? Erre a válasz: pontosan (a,m)-et. Ha több megoldás is van, azaz $(a,m) > 1$, akkor a kongruenciát és a modulust is végigosztva ezzel az (a,m) számmal kapjuk, hogy $Ax = B \pmod{M}$ valamilyen A, B, M számokra. Itt már $(A,M) = 1$ teljesül, érvényes tehát az Euler-Fermat tétel, azaz $A^{\varphi(M)} \equiv 1 \pmod{M}$. Ilyenkor beszorozva mindkét oldalt $A^{\varphi(M)-1}$-gyel kapjuk, hogy $x \equiv A^{\varphi(M)-1}B \pmod{M}$, vagyis megoldottuk a kongruenciát. Az eredeti, m-re vonatkozó kongruencia megoldásai pedig $x \equiv A^{\varphi(M)-1}B \pmod{m}$, $x \equiv A^{\varphi(M)-1}B + M \pmod{m}$, $x \equiv A^{\varphi(M)-1}B + 2M \pmod{m}$,..., $x \equiv A^{\varphi(M)-1}B + ((a,m)-1)M \pmod{m}$. A gyakorlati életben $A^{\varphi(M)-1}$ számítása nagyon sok számolást is igényelhet.

   Megoldandó a $4x \equiv 2 \pmod{6}$ lineáris kongruencia. Megoldhatóság: $(4,6)|2$ teljesül, tehát megoldható. A megoldásszám: $(4,6) = 2$. Gyakorlaton négyféle módszert tanultunk az ilyen kongruenciák megoldására:

   - 1. A naív módszer. Végigpróbálgatjuk az összes 6-os maradékosztályt, hogy megoldás-e. $x \equiv 0$-ra $4x \equiv 0 \not\equiv 2 \pmod{6}$. $x \equiv 1$-re $4x \equiv 4 \not\equiv 2 \pmod{6}$. $x \equiv 2$-re $4x \equiv 8 \equiv 2 \equiv 2 \pmod{6}$. Tehát ez egy megoldás. $x \equiv 3$-ra $4x \equiv 12 \equiv 0 \not\equiv 2 \pmod{6}$. $x \equiv 4$-re $4x \equiv 16 \equiv 4 \not\equiv 2 \pmod{6}$. $x \equiv 5$-re $4x \equiv 20 \equiv 2 \equiv 2 \pmod{6}$. Tehát ez a másik megoldás. A módszer előnye: kis modulus esetén gyors és fájdalommentes siker. Hátrány: nagy modulus esetén nagyon sokáig tart. Ha találtunk annyi megoldást, mint amennyi a megoldásszám, akkor nem kell tovább próbálgatni, több megoldás ugyanis nem lesz.
   - 2. Ügyeskedések. Osszunk le 2-vel, hogy az egyszerűbb $2x \equiv 1 \pmod{3}$ kongruenciához jussunk. Ezt kell megoldani. Vegyük észre hogy csökkent a megoldásszám, mert most már $(2,3) = 1$. Folytatva az ügyeskedést $-x \equiv 1 \pmod{3}$ végül $x \equiv -1 \equiv 2 \pmod{3}$. A kapott megoldásból vissza kell nyerni az eredeti kongruencia megoldásait. Ezt úgy kapjuk meg, hogy a kapott alapmegoldást eltoljuk a saját maradékosztályával (vagyis most 3-mal) annyiszor, ahány megoldás van összesen: $x \equiv 2 \pmod{6}$ illetve $x \equiv 2 + 3 \equiv 5 \pmod{6}$ a megoldások, pont mint előbb. Előny: Gyors siker akár nagy modulusok esetén is, de a módszer nem algoritmikus. Alkalmazhatósága inkább a szerencsén, illetve „jól kitalált" feladatokon múlik.
   - 3. Visszavezetés lineáris diofantikus egyenletre. $4x \equiv 2 \pmod{6}$ azt jelenti, hogy a $4x-2$ kifejezés 6-tal osztható, vagyis $4x-2 = 6y$ valamilyen y egészre. Innen $2x-1 = 3y$, vagyis megoldandó a $2x-3y = 1$ diofantikus egyenlet. Ez már algoritmikusan megy: Az x, y változók közül a kisebb együtthatót kifejezzük a nagyobb segítségével: $2x = 1 + 3y$, majd osztás után $x = y + \frac{1+y}{2}$. Mivel x, y egészek, ezért az $\frac{1+y}{2}$ tört is egész, legyen mondjuk v az értéke. Tehát $v = \frac{1+y}{2}$, vagyis megoldandó a $2v - y = 1$ diofantikus egyenlet. Vegyük észre hogy az eljárás során csökkentettük az együtthatók méreteit. Az eljárás addig megy, amíg valamelyik együttható a kapott diofantikus egyenletben 1 lesz. Ekkor $y = 2v - 1$ és így $x = y + v = 2v - 1 + v = 3v - 1$, v egész paraméter. Megvannak tehát a megoldások. Behelyettesítéssel azonnal látszik, hogy minden ilyen alakú x szám megoldása lesz a kongruenciának. Már csak azt kell kideríteni, 6-os maradék szerint milyen x-ek jöhetnek szóba. Pl. $v = 0$-ra $x = -1 \equiv 5 \pmod{6}$, és $v = 1$-re $x = 2 \equiv 2 \pmod{6}$ adódik. A két megoldást megtaláltuk, több megoldás nincs. Előny: algoritmikus. Nagy modulusok esetén ez az egyetlen járható út. Hátrány: sok számolás.
   - 4. A moduláris invertálás módszere. Megoldandó a $4x \equiv 2 \pmod{6}$ kongruencia. Jó volna az x együtthatóját eltüntetni, mégpedig úgy, hogy a 4 „inverzével" beszorzunk. Igen ám, de a négynek mod 6 nincs inverze. (Gondoljunk bele: ha lenne ilyen inverz, akkor azzal beszorozva egyetlen megoldást kapnánk. Na de lehet hogy nincs is megoldás, vagy az is lehet, hogy több megoldás van). Ezért prekondicionáljuk a feladatot, és leosztunk annyival, hogy az x együtthatója, és az így nyert új modulus már relatív prímek legyenek. Ehhez $(4,6) = 2$-vel kell osztani. Kapjuk: $2x \equiv 1 \pmod{3}$. Most már egyértelmű a megoldás, és van moduláris inverz is. Ez nem más, mint $2^{\varphi(3)-1}$, ezzel beszorozva mindkét oldalt, a bal oldal így alakul: $2 \cdot 2^{\varphi(3)-1}x = 2^{\varphi(3)}x \equiv 1 \cdot x$. A jobb oldalon pedig $1 \cdot 2^{\varphi(3)-1} = 2^{\varphi(3)-1}$ áll. $\varphi(3) = 2$, így kapjuk, hogy $x \equiv 2^{2-1} \equiv 2 \pmod{3}$. A két megoldás tehát $x \equiv 2 \pmod{6}$ illetve ennek eltoltja: $x \equiv 2 + 3 \equiv 5 \pmod{6}$.

3. *Számelméleti függvények.* Mely számokra igaz, hogy $d(n) = \varphi(n) = 4$? Írjuk fel n-t kanonikus alakban $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Érdemes először a $d(n)$ függvényt nézni: $d(n) = (1+\alpha_1)\dots(1+\alpha_r) = 4$. A kérdés: hogyan írható fel a 4 mint egész számok szorzata? Kétféleképpen: 1·4 vagy 2·2. Tehát vagy $\alpha_1 = 3$ és így $n = p^3$ vagy $\alpha_1 = 1, \alpha_2 = 1$ és így $n = pq$. Még arra volna szükség, hogy $\varphi(n) = 4$ is teljesüljön. Az első esetben $\varphi(n) = \varphi(p^3) = p^3(1-\frac{1}{p}) = p^3 - p^2 = p^2(p-1) = 4$, és innen $p = 2$, vagyis $n = 2^3 = 8$ adódik. A másik esetben $\varphi(n) = \varphi(pq) = pq(1-\frac{1}{p})(1-\frac{1}{q}) = (p-1)(q-1) = 4$. Ismét azt kell vizsgálni, hogy a 4 hogyan írható fel egész számok szorzataként. Vagy $p-1 = 1$ és $q-1 = 4$ és ekkor $p = 2$ és $q = 5$, és így $n = 10$ vagy pedig $p-1 = 2$ és $q-1 = 2$ vagyis $p = q = 3$, de ez nem megoldás, mert p és q különböző prímek. Az összes ilyen szám tehát a 8 és a 10.

4. *Az Euler-Fermat tételre alkalmazás.* A kulcsszó az ilyen típusú feladatok felismerésére a *végtelen sok*. Példa: mutassuk meg, hogy 7-nek végtelen sok hatványa végződik 7-re. Megoldás: 10-es maradékokat kell nézni. Mivel $(7, 10) = 1$, az Euler-Fermat tétel szerint $7^{\varphi(10)} \equiv 1 \pmod{10}$. Tehát van egyetlen egy hatvány (a $\varphi(10) = 10(1-\frac{1}{2})(1-\frac{1}{5}) = 4$), amelyre a 7-et emelve 1 végződést kapunk. Ha az előző kongruenciát valamilyen k hatványra emeljük, akkor azt látjuk, hogy a $k\varphi(10)$ hatványok is mind-mind olyanok, amelyek 1-re végződnek. Nekünk 7-es végződés kell, hát szorozzuk be ezeket a számokat 7-tel, kapjuk, hogy $7^{\varphi(10)k+1} \equiv 7 \pmod{10}$ azaz a 7 minden $4k+1$ alakú hatványa minden pozitív egész k esetén 7-re végződik.

5. *Csoportaxiómák ellenőrzése.* Négy dolgot kell megnézni: zártság, asszociativitás, egységelem, inverz. Példa: Igaz-e, hogy a 2×2-es valós elemű, 1 determinánsú mátrixok csoportot alkotnak a mátrixok szokásos összeadására, mint műveletre nézve? A zártság ellenőrzésekor azt a kérdést teszi fel magának az ember, hogy „igaz-e, hogy két valós elemű, 1 determinánsú mátrix összege is ilyen?”. A válasz nyilván nemleges, az ellenpéldát a

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} \frac{3}{2} & 0 \\ 0 & 3 \end{bmatrix}$$

egyenlőség mutatja, ahol bár a két bal oldalon lévő mátrix egységnyi determinánsú, a jobb oldali már nem. Tehát a művelet nem zárt a halmazra, tehát a sturktúra nem csoport. Példa: A valós számpárok halmazán legyen értelmezve egy új $\oplus$ művelet a következőképpen:

$$(a, b) \oplus (c, d) := (ac - bd, bc + ad)$$

Csoportot kapunk-e így? Zártság: valós számpárok eredménye valós számpár, tehát a művelet zárt. Asszociativitás:

$$((a, b) \oplus (c, d)) \oplus (e, f) = (ac - bd, bc + ad) \oplus (e, f) = (ace - bde - bcf - adf, bce + ade + acf - bdf)$$

$$(a, b) \oplus ((c, d) \oplus (e, f)) = (a, b) \oplus (ce - df, de + cf) = (ace - adf - bde - bcf, bce - bdf + ade + acf)$$

Egységelem: Kell olyan (E, F) számpár, ami minden mást fixen hagy, nevezetesen:

$$(a, b) \oplus (E, F) = (E, F) \oplus (a, b) = (a, b)$$

$$(aE - bF, bE + aF) = (Ea - Fb, Fa + Eb) = (a, b)$$

Itt az első egyenlőség igaz, megoldandó tehát a $aE - bF = a$, $bE + aF = b$ egyenletrendszer. Ennek teljesülnie kell $(a, b) = (1, 0)$-ra is, vagyis $E = 1, F = 0$, vagyis az egységünk az $(1, 0)$. Lehet ellenőrizni, hogy ez tényleg minden (a, b) számpárt fixen hagy. Inverz: Minden (a, b) számpárhoz le kellene gyártani egy (A, B) számpárt, az ő inverzét, amellyel összeadva a $\oplus$ művelettel az egységelem, vagyis $(1, 0)$ adódik.

$$(a, b) \oplus (A, B) = (A, B) \oplus (a, b) = (E, F) = (1, 0)$$

Átírva:

$$(aA - bB, bA + aB) = (Aa - Bb, Ba + Ab) = (1, 0)$$

Itt az első egyenlőség mindig teljesül. Megoldandó tehát minden (a, b) paraméterre az $Aa - Bb = 1$ $Ba + Ab = 0$ egyenletrendszer. Az $(a, b) = (0, 0)$ párra azonban $0 = 1, 0 = 0$ ellentmondó egyenlet adódik. Tehát ennek az elemnek nincs inverze, a struktúra a művelettel nem alkot csoportot.

6. *Absztrakt algebrai feladat.* Sokféle feladat elképzelhető, megoldásukra nincs semmiféle általános módszer. Fontos tudni, hogy kell egy Cayley-tábláról leolvasni információkat (pl. melyik elem az egységelem, mi egy algebrai kifejezésnek, pl. ab^2c^3-nek a csoportbeli eredménye. Előfordulhat Diéder-csoportos feladat.