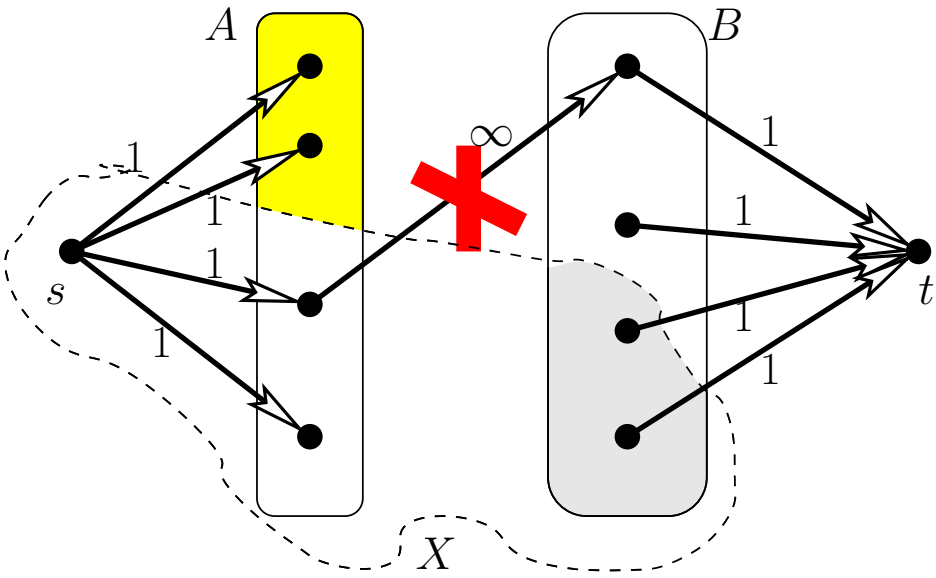
Bevezetés a számításelméletbe II.

A BME informatikus-hallgatói számára

segédlet a 2006. tavaszi VISZA 110 előadáshoz

Összeállította: Fleiner Tamás



Tartalomjegyzék

Bevezetés

Ez a jegyzet a BME-n, a 2005/2006-os tanév második félévében az informatikus-hallgatók számára előadott „Bevezetés a számításelméletbe II." c. előadáshoz kapcsolódik, és elsősorban az említett tárgyból történő vizsgára való felkészülés segédanyaga. Nem pótolja azonban a rendelkezésre álló, könyvformátumú jegyzetet, amellyel számos tekintetben egyezik. Előnye talán mégis annyi, hogy szorosabban kapcsolódik az órán leadott anyaghoz, és így koncentráltabban tartalmazza a vizsgán számonkért tudást. Jelen jegyzet valamennyire túl is mutat azonban az előadáson elhangzottakon, így olyan részeket is tartalmaz, amik nem hangzottak el az előadáson, illetve amiket nem kérünk számon a vizsgán. Ha tehát valaki egészen véletlenül komolyabban érdeklődik egy-egy témakör iránt (bár, őszintén szólva, szkeptikus vagyok ezzel kapcsolatban), azok számára odabiggyesztettem néhány, általam érdekesnek ítélt megjegyzést. Ezek lábjegyzetben[1] ill. apró betűs szedéssel olvashatóak. Ne felejtsük el azonban, hogy ezek csupán a tananyagot kiegészítő megjegyzések: ahhoz, hogy egy adott anyagrészben valaki ténylegesen elmélyülhessen, a megfelelő szakirodalmat (is) célszerű tanulmányoznia.

A bizonyítások végét olyan kiskocka jelzi, mint amilyen pl. ebben a sorban is áll. □

Hogyan is jött létre a jegyzet? Egy előadássorozat tervezésekor az előadónak célszerű saját használatára vázlatot készítenie az elhangzó anyagról, hogy az minél egységesebb és szervesebben felépülő lehessen. Hála a korszerű technológiák elharapózásának, immár ott tartunk, hogy nem lényegesen bonyolultabb egy ilyesfajta anyagot digitálisan szerkeszteni ill. tárolni, mint a hagyományos papíralapon[2]. A jegyzet elsősorban tehát az előadó saját segédanyagaként került összeállításra. Ennek egy következménye, hogy a stílus meglehetősen tömör. Nem kell meglepődni, ha egy-egy mondat teljes megértéséhez akár több dolgot is át kell gondolni. Szerencsére nem bukkannak fel lépten-nyomon ilyen mondatok.

Minden erőfeszítés ellenére valószínűleg számos hiba maradt az alábbi jegyzetben. Lehetne persze több is. Szerencsére voltak, akik segítettek. Úgyogy köszönetet mondok mindenkinek, aki részt vett az anyag javításában, köztük számos villamosmérnök-hallgatónak, akik a jegyzet korábbi verziójában éktelenkedő problémákra hívták fel a figyelmem. Természetesen minden megmaradt hibáért a felelősség egyedül a szerzőé. Az ezekkel kapcsolatos megjegyzéseket és a konstruktív hozzászólásokat köszönettel fogadom a `fleiner@cs.bme.hu` címen.

Jelen jegyzet jelentős része szellemi termék, és nemcsak a szerzőé. Terjeszti a BME Számítástudományi és Információelméleti Tanszéke, forgalombahozatala önköltségi áron történik. A szerzői jogok tekintetében a szerző elképzelései az alábbiak. A jegyzet jelenlegi formájában másolható, terjeszthető, de kizárólag a szerző és a forrás pontos megjelölésével és ingyenesen. Ugyanez a megkötés öröklődjék minden olyan szerzői jog hatálya alá eső dologra, ami a jelen munka fenti típusú felhasználása során származik. Az emítettől eltérő célú felhasználáshoz (pl. a jegyzet szerkesztéséhez, átdolgozásához, árusításához) jelen munka szerzőjének engedélye szükséges.

A jegyzet reményeim szerint karbantartott változata a `www.cs.bme.hu/~fleiner/bsz052` weblapról tölthető le.

Minden olvasónak sikeres felkészülést és eredményes vizsgázást kívánok.

Budapest, 2006. május 10.

Fleiner Tamás

[1] Mint pl. ez is, itt.

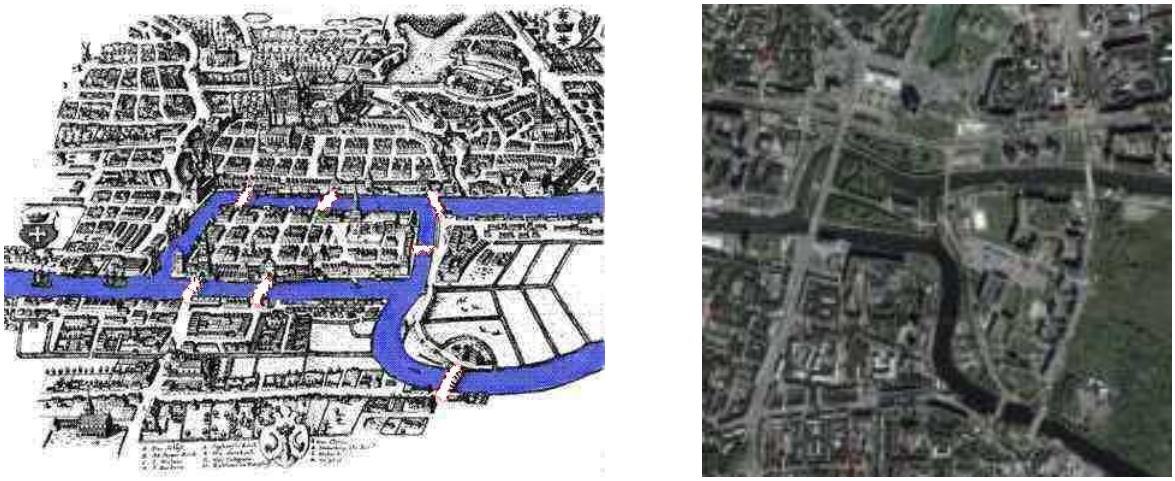
[2] illetve dehogyisnem... Valaha egy vázlatos anyag volt a jegyzet őse: akkor ez még (többé-kevésbé) igaz volt rá. Később elkezdett bővülni, és egyre inkább jegyzetformája lett. Na ez már egy pinduri kis szöszmötöléssel járt.

1. Euler és Hamilton bejárások

Def: A $G = (V, E)$ gráf *Euler-útja (Euler-köre)* a G gráf egy olyan (zárt) élsorozata, amely G minden élét pontosan egyszer tartalmazza.

Voltaképpen a G gráf éleinek olyan bejárásáról van szó, melyben minden élt pontosan egyszer érintünk. A rejtvényújságokban szokásos „rajzoljuk le egy vonallal, a ceruza felemelése nélkül" típusú fejtörő absztrakt változata: ha a lerajzolandó ábrát egy (síkbarajzolt) gráfnak tekintjük, melynek csúcsai az ábra csomópontjai, élei pedig a csomópontok között futó ívek, akkor pontosan abban az esetben oldható meg a feladvány, ha létezik az említett gráfnak Euler-útja.

A gráfelmélet születésének a „Königsbergi hidak problémájának" megoldását szokás tekinteni. Történt ugyanis, hogy 1736-ban Leonard Euler megválaszolta városa, a porosz Königsberg polgárait izgalomban tartó kérdést, miszerint miért nem sikerül száraz lábbal olyan sétát tenniük, melyben a Pregolia folyó hét hídjának mindegyikén pontosan egyszer haladnak át, és mindeközben vízijárművet nem vesznek igénybe.



1. ábra. Königsberg a XVIII. században, és Kalinyingrád a XXI.-ben.

Euler megfigyelte, hogy az egyes szárazföldeket csúcsoknak, a hidakat pedig közöttük futó éleknek tekintve éppen egy minden élt pontosan egyszer tartalmazó élsorozat létezése a kérdés. A konkrét esetben pedig nem teljesül az alább következő szükséges feltétel.[3]

Állítás: Ha a véges G gráfnak létezik Euler-köre, akkor G minden csúcsának páros a fokszáma. Ha G-ben létezik Euler-út, akkor G-nek 0 vagy 2 páratlan fokú csúcsa van.

Biz: A séta éleit az azokon való áthaladás szerint irányítva minden csúcs befoka azonos lesz a kifokával, kivéve esetleg az első és utolsó csúcsot. A fokszám pedig a kifok és befok összege, tehát ahol ezek egyenlőek, ott páros. □

Az iménti szükséges feltételnek az értelmes megfordítása is igaz.

Tétel: [4] Ha a $G = (V, E)$ gráf véges és összefüggő, akkor

1. G-nek pontosan akkor van Euler-köre, ha G minden csúcsa páros fokú, ill.
2. G-nek pontosan akkor van Euler-útja, ha G-nek 0 vagy 2 páratlan fokú csúcsa van.

Biz: 1.: A szükségesség a fenti megfigyelésből következik. Az elégségességet G élszáma szerinti indukcióval bizonyítunk. 0-élű gráfokra a tétel nyilvánvalóan igaz. Tegyük fel, hogy m-nél kevesebb élű gráfokra a tételt már bebizonyítottuk, és legyen G-nek m éle.

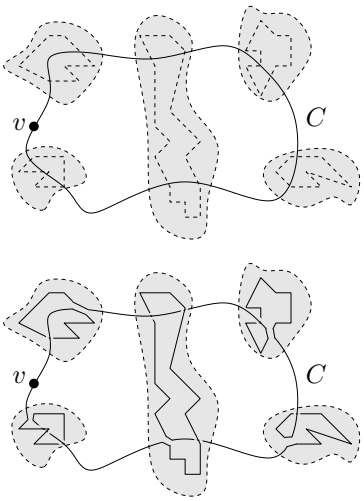
[3] Jegyezzük meg, hogy Königsberg mai neve Kalinyingrád, és a Kalinyingrádi Orosz Exklávé székhelye. Az exklávé annyit tesz, mint Oroszország olyan összefüggő komponense, mely nem tartalmazza Moszkvát. Szomszédai Litvánia és Lengyelország, így 2004 óta az EU veszi körül Oroszország egy részét. Kalinyingrád stratégiai jelentősége abból fakad, hogy ez az Orosz Föderáció az egyetlen fagymentes északi kikötője, a szovjet balti flotta korábbi állomáshelye.

Königsberg tehát a gráfelmélet bölcsőjének tekinthető. A matematika szempontjából azonban nemcsak emiatt fontos, hiszen szülötte volt a számelmélész Christian Goldbach (akinek sejtésére később térünk ki), a geométer David Hilbert de a számelmélettől a Fourier-analízisig számos területet művelő Rudolf Lipschitz és még sokan mások is. A város a korabeli szellemi életnek szintén az egyik központja volt: innen származik például a filozófus Immanuel Kant és a fizikus Gustav Kirchhoff, utóbbiról szintén szó lesz nemsokára.

Eulerről egy érdekes tény még, hogy ha a ma kombinatorikával foglalkozó matematikusoknál megvizsgáljuk ki volt a doktori témavezetőjének a doktori témavezetőjének a ... stb, akkor az esetek jelentős részében Leonard Eulerig jutunk: a jelen jegyzet szerzője is az ő köbükunokája. A hidakra visszatérve említést érdemel még, hogy a korabeli hét hídból kettő már nem áll, épült viszont másik kettő, melyek egészen más szárazföldeket kötnek össze. A kalinyingrádi hét híd bejárása ennek ellenére továbbra sem lehetséges: a jelenlegi gráf izomorf az Euler korabelivel. (Ld. az ábrát)

[4] Az egyik első gráfelmélettel foglalkozó könyvben a tétel első része így szerepel: Egy véges G gráfnak akkor és csak akkor van Euler-köre, ha G összefüggő és páros. Tanulságos meggondolni, miért is nem igaz ez az állítás.

G-ben létezik egy C kör, mert minden fokszám legalább kettő: ha elindulunk G egy tetszőleges csúcsából, és mindig csatlakozó éleken lépünk tovább, akkor egyszer egy korábban érintett v csúcsba kell jutnunk, hisz elsőfokú pont híján sosem akadhatunk el. A v csúcs két érintése között pedig éppen egy kört jártunk be.



Tekintsük a $G' = G - C$ gráfot, mely C éleinek törlésével keletkezik G-ből. G' minden egyes komponense véges, öf, m-nél kevesebb élt tartalmaz, és minden fokszáma páros, ezért az indukciós feltevés miatt minden komponensnek van Euler-köre. A G Euler-körét úgy kapjuk, hogy C egy v csúcsából indulva C élein haladunk végig, azonban mikor egy nemtriviális komponensbe érkezünk, akkor az adott komponens Euler-köre szerint haladunk tovább, majd miután azzal végeztünk, folytatjuk a C kör bejárását. (Itt felhasználtuk, hogy ha egy komponensnek van Euler-köre, akkor van olyan Euler-köre is, aminek kezdő- (és így végpontja) a komponens egy adott csúcsa.) A kapott élsorozat nyilván G Euler-köre lesz.

2.: Ha G minden csúcsának foka ps, akkor 1. miatt létezik Euler-kör, ami egyúttal Euler-út is. Egyébként húzzunk be G ptn fokú csúcsai között egy új e^* élt. 1. miatt a keletkező G' gráfnak létezik Euler-köre, feltehetjük, hogy e^* a kör utolsó éle. Az e^* él Euler-körből való törlésekor éppen G egy Euler-útját kapjuk. □

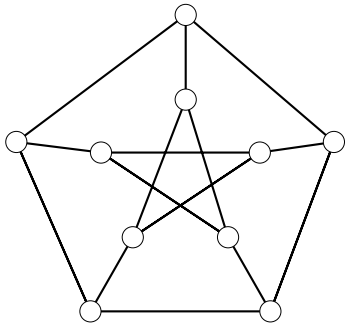
Def: A G gráf *Hamilton-köre (Hamilton-útja)* a G olyan köre (útja), mely G minden csúcsát tartalmazza.

Megjegyzés: Mivel egy körben (útban) szereplő minden csúcs különböző, ezért a Hamilton-kör (Hamilton-út) a G gráf olyan bejárása, mely G minden csúcsát *pontosan* egyszer érinti.

Állítás: Ha a véges G gráfban létezik Hamilton-kör (ill. Hamilton-út), akkor G-nek k tetszőleges pontját törölve, a keletkező gráfnak legfeljebb k (ill. $k+1$) komponense van.

Biz: Ha a G gráf maga egy Hamilton-kör (Hamilton-út), akkor az állítás világos. Ha G-nek további élei is vannak, akkor a pontok törlése után keletkező komponensek száma csak csökkenhet. □

Megjegyzés: A fenti állítás egy szükséges, ám nem elégséges feltétel. A Petersen-gráfnak nincs Hamilton-köre, noha teljesíti a feltételt. Ha volna Hamilton-köre, akkor 3 színnel színezhetnénk az éleit úgy, hogy az azonos színű élek pként diszjunktak legyenek. (A Hamilton-kör 10 élére kell 2 szín, a kimaradó élek pedig diszjunktak, mivel a Petersen-gráf 3-reguláris.) Márpedig a külső ötszög és a hozzá csatlakozó élek 3-színezése (a szimmetria miatt) lényegében egyértelmű, és ez nem terjeszthető ki globális 3-színezéssé.



A Petersen-gráf

Ha a Petersen-gráf külső köréből a, belső köréből pedig b csúcsot hagyunk el, akkor a külső ill. belső körön keletkező komponensek száma legfeljebb a ill. b, vagyis a gráfnak nem keletkezhet összességében $a+b$-nél több komponense.

Vannak azonban jól használható, elégséges feltételek is Hamilton-kör létezésére.

Dirac tétele: Ha az n-pontú ($n \geq 3$), egyszerű G gráf minden pontjának foka legalább $\frac{n}{2}$, akkor G-nek van Hamilton-köre.

Ore tétele: Ha az n-pontú ($n \geq 3$), egyszerű G gráf olyan, hogy $uv \notin E(G)$ esetén $d(u) + d(v) \geq n$, akkor G-nek létezik Hamilton-köre.

Megjegyzés: Ha egy gráfra teljesül a Dirac feltétel, akkor teljesül rá az Ore is. Ezért a Dirac tétel következik az Ore tételből.

Pósa tétele: Ha az n-pontú ($n \geq 3$), egyszerű G gráf fokszámai $d_1 \leq d_2 \leq \ldots \leq d_n$, és minden $k < \frac{n}{2}$ esetén $d_k \geq k+1$, akkor G-nek létezik Hamilton-köre.

Állítás: Ha egy gráfra teljesül az Ore feltétel, akkor teljesül rá a Pósa is. Ezért az Ore tétel következik a Pósa tételből.

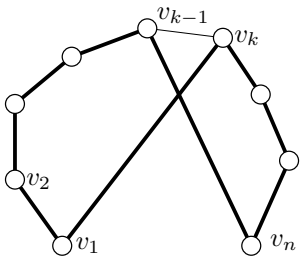
Biz: Indirekt. Legyen $d_k \leq k$ valamely $1 \leq k < \frac{n}{2}$-re, és legyen U a k legkisebb fokú pont halmaza. Bármely U-beli pont fokszáma legfeljebb k, így bármely két U-beli pont fokszámösszege kisebb, mint n, ezért az Ore feltétel miatt U teljes gráfot feszít. Minden U-beli pontból tehát $k-1$ él indul U-beli ponthoz, ezért legfeljebb 1 él indulhat U-n kívülre. $k < \frac{n}{2}$ miatt létezik tehát $V(G) \setminus U$-nak olyan v pontja, mely U egyetlen pontjával sincs összekötve. Ekkor tetszőleges $u \in U$ csúcsra u és v fokszámösszege legfeljebb $k + (n-k-1) = n-1$, ami ellentmond az Ore feltételnek.

Chvátal tétele: Legyen G n-pontú ($n \geq 3$), egyszerű gráf, melynek fokszámai $d_1 \leq d_2 \leq \ldots \leq d_n$. Tegyük fel, hogy minden olyan $k < \frac{n}{2}$-re, melyre $d_k \leq k$ teljesül, fennáll a $d_{n-k} \geq n-k$ egyenlőtlenség. Ekkor G-nek létezik Hamilton-köre.

Másrészt, ha a $d_1 \leq d_2 \leq \ldots \leq d_n$ fokszámsorozatra nem teljesül az előző feltétel, akkor van olyan gráf, melynek nincs Hamilton-köre, és $d'_1 \leq d'_2 \leq \ldots \leq d'_n$ fokszámsorozatára teljesül, hogy $d_i \leq d'_i \ \forall i = 1, 2, \ldots, n$.

Megjegyzés: Ha egy gráfra teljesül a Pósa feltétel, akkor teljesül rá a Chvátal is. Ezért a Pósa tétel következik az Chvátal tételből.

Az Ore tétel bizonyítása: Legyenek G egy ellenpélda a tételre. Mivel új élek behúzása nem rontja el az Ore-tulajdonságot, feltehetjük, hogy G-ben bármely új él behúzása létrehoz egy Hamilton-kört, azaz G bármely két összekötetlen pontja között vezet Hamilton-út. Ha tehát u és v nem szomszédosak, akkor létezik egy P Hamilton-út u-ból v-be, feltehetjük, hogy ez az út az $u = v_1, v_2, v_3, \ldots, v_n = v$ sorrendben tartalmazza G csúcsait. Ha most v_1v_k a G gráf éle, akkor $v_{k-1}v_n$ nem lehet G éle, mert $v_1, v_2, \ldots, v_{k-1}, v_n, v_{n-1}, v_{n-2}, \ldots, v_k, v_1$ egy Hamilton-kör lenne, ellentétben G választásával.



Ha tehát v_1 szomszédai a $v_{i_1}, v_{i_2}, \ldots, v_{i_m}$ csúcsok, akkor v_n-nek nem lehet szomszédja a $v_{i_1-1}, v_{i_2-1}, \ldots, v_{i_m-1}$ csúcsok egyike sem, azaz v_n szomszédainak száma legfeljebb $n-1-m$ lesz, vagyis $d(v_1) + d(v_n) \leq m + n - 1 - m = n - 1 < n$, ellentmondás. □

A Chvátal tétel bizonyítása: Feltehetjük, hogy G csúcsai az $1, 2, \ldots n$ pontok, és $d(1) \leq d(2) \leq \ldots \leq d(n)$. Indirekt bizonyítunk, legyen G egy ellenpélda a tételre. Mivel új élek behúzása nem rontja el a Chvátal-tulajdonságot, feltehetjük, hogy G-ben bármely új él behúzása létrehoz egy Hamilton-kört, azaz G bármely két összekötetlen pontja között vezet Hamilton-út. Ha tehát k és l nem szomszédosak, akkor az P_{kl} Hamilton-úton a k szomszédait megelőző pontok V_{kl} halmazából nem futhat él l-be, mert akkor lenne G-ben Hamilton-kör. Ezért (figyelembe véve, hogy $k \in V_{kl}$) $d(k) + d(l) \leq d(k) + (n-1) - d(k) = n - 1$ teljesül. (Ez idáig tkp az Ore tétel bizonyítása.)

Válasszuk most a nem szomszédos k, l pontokat úgy, hogy $d(k)+d(l)$ maximális legyen. (Világos, hogy $d(k) \leq \frac{1}{2}(d(k)+d(l)) \leq \frac{n-1}{2} < \frac{n}{2}$.) Mivel nem V_{kl} pontjait választottuk k helyett, ezért $d(i) \leq d(k)$ áll minden $i \in V_{kl}$-re. Eszerint $d(d(k)) \leq d(k)$, így a Chvátal feltétel miatt $d(n - d(k)) \geq n - d(k)$ áll, vagyis G-nek legalább $d(k)+1$ olyan pontja van, mely legalább $n - d(k)$-fokú. $d(k) < \frac{n}{2}$ miatt van tehát e pontok között egy l', mely nem szomszédja k-nak, de ekkor $d(k) + d(l') \geq d(k) + n - d(k) = n > d(k) + d(l)$, ellentmondásban l választásával. □

Megjegyzés: Ha csak a fokszámsorozat alapján kell megmondani, van-e biztosan Hamilton-kör a gráfban, akkor nem állíthatunk erősebbet a Chvátal tételénél. Tetszőleges $n \in \mathbb{N}$-re és tetszőleges $k < \frac{n}{2}$-re létezik ugyanis olyan n-pontú, egyszerű gráf, melynek nincs Hamilton-köre, de k db k-adfokú, $(n-2k)$ db $(n-k-1)$-edfokú és k db $(n-1)$-edfokú pontja van. (Az innen adódó fokszámsorozat csak k-ra sérti meg a Chvátal feltételt. Bármely fokszám megnövelésével pedig teljesül a Chvátal feltétel.) Legyenek ugyanis az A, B, C ponthalmazok rendre k, k ill. $n-2k$ pontúak, húzzuk be C-n belül az összes élt, továbbá kössük össze B minden pontját az összes többi ponttal. A fokszámok a fentiek lesznek, de B elhagyásával $k+1$ komponens keletkezik, nem található tehát a gráfban Hamilton-kör.

2. Hálózati folyamok

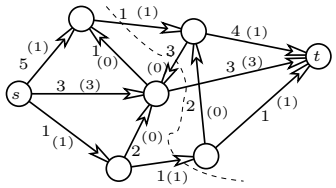
A továbbiakban olyan irányított gráfokat vizsgálunk, melyek minden éléhez tartozik egy, az adott élt valamilyen szempontból jellemző szám. Az ilyen, számozott élekkel rendelkező gráfok több gyakorlati probléma esetén nagyon természetesen bukkannak fel, elég itt az algoritmuselméletből később tanult PERT problémára utalni. Mi itt most egy másik modellel foglalkozunk. *Hálózatnak* nevezünk egy olyan (G, s, t, c) négyest, amelyben G egy irányított gráf, aminek s és t különböző csúcsai, továbbá G minden e élét jellemzi egy nemnegatív $c(e)$ szám, az e él ú.n. *kapacitása*. Nem követelmény, hogy a G gráf aciklikus legyen: irányított köröket is megengedünk.

A G gráfot szemléletesen egy számítógéphálózat modelljének gondolhatjuk: G minden csúcsa egy-egy számítógép, és az s csúcsban található számítógépről szeretnénk információt küldeni a t csúcsbelibe. Az irányított élek a gépeket összekötő, kommunikációs csatornáknak felelnek meg. Minden ilyen csatornán csak egy irányba küldhető információ, továbbá minden csatornának adott a maximális sávszélessége is. Egy más személet alapján egy csőhálózat modelljének tekinthető a hálózat, ahol s-ben tápláljuk a hálózatba a t-be szállítandó folyadékot. A csúcspontok közötti kapcsolatot reprezentáló élek itt egy-egy csőnek felelnek meg, melynek $c(e)$ kapacitása azt fejezi ki, mennyi folyadékot lehet az adott csövön egységnyi idő alatt továbbítani. (A hasonlat annyiban sántít, hogy egy szokványos csövön bármerre lehet a folyadékot szállítani, míg a modellbeli irányított élek ezt csak egy irányba engedik meg. Azonban ha G minden irányított élének ellenkező irányítású párja is ugyanakkora kapacitású éle G-nek, akkor ez már valóban a kétirányú csőhálózat egy lehetséges modellje lesz. Ilyen értelemben tehát az irányított gráfmodell általánosabb a csőhálózatnál.) Természetes kérdés, hogy az adott kapacitáskorlátok mellett mennyi a hálózat átbocsátóképessége, azaz egységnyi idő alatt mennyi információ ill. folyadék juthat s-ből t-be.[5]

A (G, s, t, c) hálózatban *folyamnak* mondunk tehát egy olyan f függvényt, mely G minden éléhez egy számot rendel úgy, hogy

[5]Ebben a bekezdésben az apró betű arra utal, hogy bár hasznos dolog szemléletes jelentést tulajdonítani a vizsgált hálozati modellnek, mindez nem elegendő a folyamok és az azt követő (Menger, párosítások) anyagrész elvárt szintű megértéséhez. Tapasztalatom szerint számos hallgató pusztán e szemléletes jelentés ismeretével felvértezve vág neki a vizsgának, és nem képes definiálni az absztrakt fogalmakat (úgymint **hálózat, folyam, folyamérték,** *st*-**vágás** ill. **vágás kapacitása**). Tisztelettel szeretnék mindenkit lebeszélni az efajta próbálkozásról.

1. $0 \leq f(e) \leq c(e)$ teljesül G minden e élére, továbbá
2. $\sum\{c(uv) : u \in V(G)\} = \sum\{c(vu) : u \in V(G)\}$ áll G minden, s-től és t-től különböző v csúcsára.



Hálózati folyam. A zárójelekben az f folyam által felvett értékek állnak.
A folyamérték $m_f = 1 + 3 + 1 = 5$.
A szaggatott vonal egy 5 értékű vágást jelöl.

Az első *kapacitás-feltétel* azt fejezi ki, hogy a folyam minden élen legfeljebb kapacitásnyi lehet, a második, ú.n. *Kirchhoff-szabály* azt mondja ki, hogy minden, s-től és t-től különböző v csúcsra a befolyó folyam összmennyisége azonos a kifolyó összfolyammal, tehát egyetlen csúcsban sem keletkezik vagy tűnik el folyadék. A név egyúttal arra is utal, hogy a hálózati folyam fogalma az elektromos hálózatok elméletében is hasznos segédeszköz.

Az f folyam m_f *folyamértéke* az a folyammennyiség, ami s-ből kifolyik:

$$m_f := \sum\{f(sv) : v \in V(G)\} - \sum\{f(vs) : v \in V(G)\} \ .$$

(Rendszerint nincs ok arra, hogy s-be folyam érkezzen, hiszen onnan minél többet akarunk kijuttatni, de általában nem zárhatjuk ki ezt a lehetőséget sem. Az s-t elhagyó összfolyammennyiség kiszámításához tehát le kell vonni azt, ami s-be érkezik.)

Az f folyam értékét máshogyan is kiszámíthatjuk. Legyen X a G csúcsainak egy s-t tartalmazó, de t-től diszjunkt részhalmaza. Az X és $V(G) \setminus X$ között futó éleinek halmazát a hálózat egy *st-vágásának* nevezzük. Az X által meghatározott *st-vágás kapacitása* az X-ből $V \setminus X$-be futó élek kapacitásösszege, azaz $\sum\{c(xv) : x \in X \not\ni v \in V(G)\}$. Szemlélet alapján világos, hogy az X által meghatározott st-vágás kapacitása felső korlát a lehetséges folyam értékére. Sőt, azt sem nehéz elhinni, hogy tetszőleges f folyam m_f folyamértéke meghatározható úgy, hogy az X-ből $V(G) \setminus X$-be futó éleken haladó összfolyammennyiségből levonjuk a $V(G) \setminus X$-ből X-be továbbított folyammennyiséget. Ezt a két tényt bizonyítjuk az alábbiakban.

Állítás: Ha f a (G, s, t, c) hálózat egy folyama, és $s \in X \subseteq V(G) \setminus \{t\}$, akkor $m_f = \sum\{f(xv) : x \in X \not\ni v \in V(G)\} - \sum\{f(vx) : x \in X \not\ni v \in V(G)\}$, továbbá $m_f \leq \sum\{c(xv) : x \in X \not\ni v \in V(G)\}$.

Biz: Felhasználva, hogy minden $s \neq x \in X$-re $\sum\{f(xv) : v \in V(G)\} - \sum\{f(vx) : v \in V(G)\} = 0$ és $0 \leq f(uv) \leq c(uv)$, kapjuk, hogy

$$m_f = \sum\{f(sv) : v \in V(G)\} - \sum\{f(vs) : v \in V(G)\} = \sum_{x \in X}(\sum\{f(xv) : v \in V(G)\} - \sum\{f(vx) : v \in V(G)\}) =$$

$$= \sum_{x \in X}(\sum\{f(xv) : v \in V(G) \setminus X\} - \sum\{f(vx) : v \in V(G) \setminus X\}) =$$

$$= \sum\{f(xv) : x \in X \not\ni v \in V(G)\} - \sum\{f(vx) : x \in X \not\ni v \in V(G)\} \leq \sum\{c(xv) : x \in X \not\ni v \in V(G)\} \square$$

Az st-vágás tehát egy kézenfekvő eszköz annak bizonyítására, hogy a folyamérték nem lehet nagyobb egy adott mennyiségnél. Valójában ennél jobb bizonyíték nem is kell: a maximális folyamérték pontosan megegyezik a minimális vágáskapacitással. Ezt mondja ki az alábbi „max-flow min-cut" (MFMC) tétel.

Ford-Fulkerson tétel: Ha (G, s, t, c) egy véges hálózat, akkor létezik egy f folyam és egy $s \in X \subseteq V(G) \setminus \{t\}$ részhalmaz úgy, hogy az m_f folyamérték azonos az X által definiált st-vágás kapacitásával.

Biz: Először (a rend kedvéért) igazoljuk, hogy létezik maximális folyam, azaz olyan f folyam, melyre $m_f \geq m_{f'}$ minden f' folyamra. Nyilván az $X = \{s\}$ által meghatározott vágás véges kapacitása felső korlát a lehetséges folyamértékekre. A lehetséges folyamértékek x szuprémuma tehát véges. Azt kell megmutatni, hogy létezik x értékű folyam. A szuprémum definíciója miatt léteznek $f_1, f_2, \ldots$ folyamok, melyekre $\lim_{n\to\infty} m_{f_n} = x$. Az f_n sorozatnak a G gráf minden e élhez van olyan részsorozata, hogy a részsorozat az e élen konvergens. Véve a részsorozatok részsorozatait, az eredeti f_n sorozatnak olyan f_{n_i} részsorozatát kapjuk, melyre teljesül, hogy G minden e élére $f_{n_i}(e)$ konvergens. Jelölje $f(e)$ az $f_{n_i}(e)$ sorozat határértékét. Mivel $0 \leq f_{n_i}(e) \leq c(e)$, ezért a rendőr-elv miatt $0 \leq f(e) \leq c(e)$, és limesz f függvényre a Kirchhoff-feltétel teljesülése hasonlóan következik. Azt kaptuk tehát, hogy f egy folyam. A folyamérték definíciójából pedig az látszik, hogy $x = \lim m_{f_n} = \lim m_{f_{n_i}} = m_f$, tehát f csakugyan egy maximális folyam.

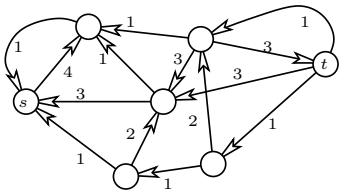
Legyen tehát f egy maximális folyam. A célunk f segítségével egy m_f kapacitású vágás megtalálása. Bevezetjük a (G_f, s, t, c_f) hálózatot a $G_f = (V(G), E_f)$ segédgráfon, melyre $E_f := E_f^{előre} \cup E_f^{vissza}$, ahol

$$E_f^{előre} := \{uv \ f(uv) < c(uv)\} \qquad E_f^{vissza} := \{vu : 0 < f(uv)\} \ .$$

G_f-nek tehát előre és visszaélei vannak: az előreélek G azon élei, melyen még tovább növelhető a folyam, a visszaélek pedig G azon éleinek a fordítottjai, melyeken a folyam pozitív, tehát csökkenthető. A G_f segédgráfon definiáljuk a

$$c_f(uv) := \begin{cases} c(uv) - f(uv) & \text{ha } uv \text{ előreél} \\ f(vu) & \text{ha } uv \text{ visszaél} \end{cases}$$

kapacitásokat. Ha tehát van egy P irányított út G_f-ben s-ből t-be (ú.n. javító út), akkor P előreélein ε-nal megnövelve f-t, P visszaéleinek megfordítottjain ε-nal csökkentve f-t egy, a Kirchhoff-szabályt teljesítő f'-t kapunk. Ha ε-t alkalmasan választjuk (nevezetesen ε a P út élein a c_f kapacitásfüggvény minimális értéke) akkor az eredeti kapacitásfeltételek is fennmaradnak, tehát f' folyam lesz, melynek folyamértéke $m_{f'} = m_f + \varepsilon > m_f$, ellentmondásban f maximalitásával.



Az előző példához tartozó (G_f, s, t, c_f) segédhálózat. (Nem tartalmaz javító utat.)

Legyen tehát X a G_f-ben s-ből elérhető pontok halmaza. A fentiek alapján $t \notin X$, azaz X egy st-vágást határoz meg. Mivel X-ből nem lép ki G_f-nek éle, ezért minden X-ből $V(G) \setminus X$-be vezető uv élre $f(uv) = c(uv)$, és minden $V(G) \setminus X$-ből X-be lépő uv élen $f(uv) = 0$. Ha tehát az előző állítás felhasználásával számítjuk ki az m_f folyamértéket az X által definiált st-vágás segítségével, akkor $m_f = \sum\{f(xv) : x \in X \not\ni v \in V(G)\} - \sum\{f(vx) : x \in X \not\ni v \in V(G)\} = \sum\{c(xv) : x \in X \not\ni v \in V(G)\}$, ami éppen az X által meghatározott st-vágás kapacitása. □

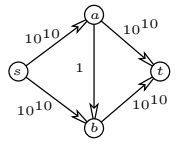
Ha a c kapacitások egészek, akkor a fenti bizonyítás egyben módszert is kínál a maximális folyam keresésére: kiindulunk az $f_0 \equiv 0$ folyamból, és elkészítjük az $f_0, f_1, f_2, \ldots$ folyamok sorozatát, melyekre $0 = m_{f_0} < m_{f_1} < m_{f_2} < \ldots$ egészek. Ha f_k-t már megtaláltuk, és f_k minden élen egész értéket vett fel, akkor a G_{f_k} segédgráfban keresünk egy P utat s-ből t-be, és f_{k+1}-t úgy kapjuk, hogy P mentén ε-nyi folyamot vezetünk, ahol ε a P élei mentén a c_{f_k} kapacitásfüggvény minimális értéke. (Pontosabban P előreélein ε-nal növeljük, visszaéleinek fordítottjain ε-nal csökkentjük f_k-t.) Eztáltal f_{k+1} is egészfolyam lesz, hisz az ε kiszámításakor bizonyos $c_{f_k}(e)$ (pozitív egész) kapacitások minimumát kellett képezni. Tehát $m_{f_k} < m_{f_{k+1}}$, és az $m_{f_{k+1}}$ folyamérték is egész. Mivel a maximális folyamértéket bármely vágáskapacitás felülről korlátozza, előbb-utóbb olyan f_l folyamot kapunk, melyen már nem tudunk a fenti eljárással javítani. Ekkor tehát nincs a G_{f_l} segédgráfban st-út, létezik tehát m_{f_l} kapacitású vágás, tehát az f_l egészfolyam egyúttal maximális folyam is. Ezzel igazoltuk az Ford és Fulkerson alábbi tételét.

Egészértékűségi lemma: Ha a (G, s, t, c) hálózatban minden e él $c(e)$ kapacitása egész szám, akkor létezik olyan maximális f folyam, hogy f a G gráf minden élén egész értéket vesz fel. □

A fenti algoritmus akkor is véges eljárás, ha nem azt kötjük ki a kapacitásokról, hogy egészek, hanem csupán annyit, hogy racionálisak. A kapacitások közös nevezőjével ugyanis mindent végigszorozva egy egészkapacitásokkal rendelkező problémát kapunk, amelyben csak véges sokszor növelhetjük legalább 1-gyel a folyamértéket. Ha azonban a c kapacitásfüggvény nem racionális, akkor még akár az is megtörténhet, hogy minden f_k-t tudunk tovább javítani, ráadásul az m_{f_k} folyamértékek nem a maximális folyamértékhez konvergálnak. Egy másik kellemetlenség, hogy a fenti, növelő utas algoritmus sokszor sajnos nem elég hatékony. Az alábbi tétel mindkét problémára megoldást kínál.

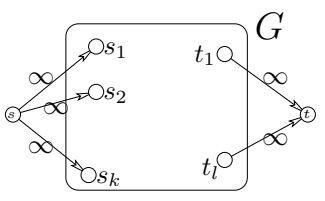
Edmonds-Karp tétel: Ha a (G, s, t, c) hálózatban a maximális folyamot a javítóutas algoritmussal keressük, és mindig egy legkevesebb élből álló javító út mentén növelünk, akkor a maximális folyam meghatározásához szükséges lépésszám felülről becsülhető $|V(G)|$ polinomjával. □

Megjegyzés: Az Edmonds-Karp tétel tehát azt biztosítja, hogy a legrövidebb javító utakon maximális mértékű javításokat végrehajtva gyorsan találjunk maximális folyamot.



Ha eszetlenül próbálunk javítani, akkor indokolatlanul sok munkába kerülhet egy maximális folyam megtalálása: az ábrán látható hálózatban felváltva az *sabt* ill. *sbat* javító utakat választva mindig csak egységnyit tudunk emelni a folyamértéken, tehát az Edmonds-Karp algoritmus által két javítás után megtalált, $2 \cdot 10^{10}$ értékű maximális folyamot csillagászati számú lépés után találjuk csak meg.

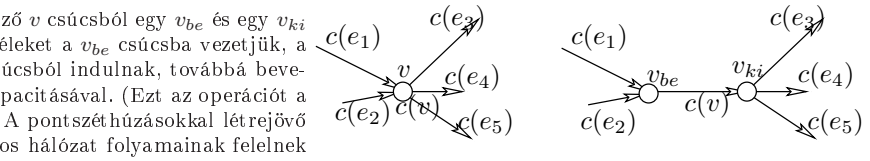
A folyamprobléma kiterjeszthető arra az esetre is, ha több forrásból több nyelőbe akarunk folyamot vezetni, de nincs megkötés arra, hogy melyik forrásból melyik nyelőbe érkezzék a folyam. Ha tehát $s_1, s_2, \ldots, s_k$ a források, $t_1, t_2, \ldots, t_l$ a nyelők, akkor bevezetünk egy-egy új s ill. t csúcsot, majd s-ből minden s_i-be ill. minden t_j-ből t-be vezetünk egy ∞ kapacitású élt[6]. Ekkor az új hálózatbeli folyamok éppen a többtermelős, többfogyasztós folyamnak felelnek meg.



Értelmezhető az a folyamprobléma is, ahol nemcsak az éleknek, hanem a pontoknak is van kapacitásuk, ami felső korlát a ponton átfolyó folyammennyiségre. Ez a probléma is visszavezethető a szokásos folyamproblémára az alábbiak szerint.

[6]Csalás! Egy hálózatban az élek kapacitása véges. A végtelen azonban itt annyit jelent, hogy olyan (véges) kapacitást adunk az adott élnek, hogy az ne legyen semminek se korlátja. Konkrétan: az ss_i él kapacitása legyen több, mint amennyi folyam az s_i-ből kifolyhat, és a $t_j t$ él kapacitása pedig legyen több annál, mint amennyi folyam t_j-be érkezhet az odavezető éleken.

Minden kapacitással rendelkező v csúcsból egy v_{be} és egy v_{ki} csúcsot képezünk: a v-be befutó éleket a v_{be} csúcsba vezetjük, a v-ből kiinduló élek pedig a v_{ki} csúcsból indulnak, továbbá bevezetünk egy $v_{be}v_{ki}$ élt a v csúcs kapacitásával. (Ezt az operációt a v pont *széthúzásának* nevezzük.) A pontszéthúzásokkal létrejövő hálózat folyamai a pontkapacitásos hálózat folyamainak felelnek meg, és viszont.



Lehetséges általánosítás még, hogy a hálózatban irányítatlan élek is vannak, melyeken bármely irányban folyhat folyam. Mint azt már a szakasz elején jeleztük, ekkor bevezetve két, ellentétesen irányított élt az irányítatlan él két végpontja között, melyek kapacitása megyegyezik az elhagyott irányítatlan él kapacitásával, akkor a probléma ismételten visszavezethető hálózati folyamokra: minden hálózati folyamnak megfelel egy folyam az irányítatlan éleket tartalmazó gráfban, és minden, az irányítatlan éleket használó folyamnak megfelelnek folyamok a hálózatban. Ha azt szeretnénk, hogy kölcsönösen egyértelmű legyen a megfeleltetés, akkor azzal a megszorítással is élhetünk, hogy a konstruált hálózatban csak olyan folyamokat nézünk, melyek rendelkeznek azzal a tulajdonsággal, hogy bármely irányítatlan élnek megfelelő két, oda-vissza irányított él közül legalább az egyiken 0 folyam folyik. A továbbiakban élni fogunk ezzel a feltevéssel.

Történelem. Ford és Fulkerson munkájának alapja az amerikai légierő számára 1955-ben készített, titkos Harris-Ross jelentés volt. Ebben a jelentésben az európai vasúti hálózatot egy 44 csúcsú, 105-élű gráffal modellezték. Az egyes csúcsok a vasúti igazgatóságoknak, az élek pedig az ezek között futó vasútvonalaknak feleltek meg. A CIA által szolgáltatott adatok alapján minden élhez egy tonnában mért kapacitást tudtak rendelni, és az így létrejött hálózatban kerestek maximális folyamot, ill. minimális vágást. A légierő érdeklődésének homlokterében természetesen a minimális vágás megtalálása állt: a hidegháború idején amerikai részről reális félelemnek tűnt a Vörös Hadsereg nyugat-európai inváziója, és ennek megállítására a logisztika hatékony rombolása tűnt az egyetlen lehetőségnek. Azon túl, hogy a titkos jelentésben megtalálják a minimális vágást (érdekesség, hogy ez Lengyelországot kettévágja, majd a Csehszlovák-Szovjet, ill. Magyar-Román határ mentén halad), be is bizonyítják, hogy ennél jobb nincs, ugyanis mutatnak egy azonos értékű folyamot is a szovjet támaszpontokból Nyugat-Európába. A légicsapások tervezéséhez a jelentés egyúttal módszert is ad egy hálózat minimális vágásának meghatározására. Ross tábornok jól értette a hadsereg működését. A jelentésben hangsúlyozta: a javasolt új módszer nem forgatja fel fenekestül az eddigi rendszert, mert a számítógépet működtető specialistákon kívül továbbra is elengedhetetlen a jól képzett katonai szakértők munkája.

Ford és Fulkerson az absztrakt hálózati modellben kimondta és bebizonyította a maximális folyam – minimális vágás tételt, ami az ezután kialakuló kombinatorikus optimalizálás tudományának egyik alappillére lett, és ezáltal jelentős hatást gyakorolt számos más tudományterületre, pl. a gráfelméletre. A jelen jegyzetben a hálózati folyamokra támaszkodva fogjuk tárgyalni a következő két fejezetet (a Menger tételek ill. páros gráfok párosításainak áttekintését), melyek történelmileg jóval korábbi eredmények, ám tárgyalásuk a hálózatok ismeretében sokkal egységesebb.

3. Menger tételei

Def: A G irányított vagy irányítatlan gráf u ponjából v pontjába futó P és Q útjait *éldiszjunktaknak* vagy *élidegennek* (*pontdiszjunktaknak* vagy *pontidegennek*) nevezzük, ha $E(P)\cap E(Q)=\emptyset$ (ill. $V(P)\cap V(Q)=\{u,v\}$). Az éldiszjunkt (pontdiszjunkt) uv utak maximális számát $\lambda(u,v)$-vel (ill. $\kappa(u,v)$-vel) jelöljük.

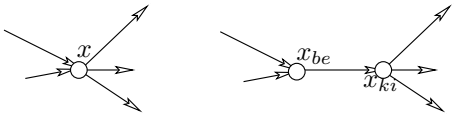
Menger tételei:

1. Ha u és v a G irányított gráf különböző csúcsai, akkor az élidegen uv utak ($\lambda_G(u,v)$-vel jelölt) maximális száma azonos az uv utakat lefogó élek minimális számával.
2. Ha u és v a G irányított gráf nem szomszédos csúcsai, akkor a pontidegen uv utak ($\kappa_G(u,v)$-vel jelölt) maximális száma azonos az uv utakat lefogó, u-tól és v-től különböző csúcsok minimális számával.
3. Ha u és v a G irányítatlan gráf különböző csúcsai, akkor az élidegen uv utak ($\lambda_G(u,v)$-vel jelölt) maximális száma azonos az uv utakat lefogó élek minimális számával.
4. Ha u és v a G irányítatlan gráf különböző csúcsai, akkor a pontidegen uv utak ($\kappa_G(u,v)$-vel jelölt) maximális száma azonos az uv utakat lefogó pontok minimális számával.

Biz: Világos, hogy a lefogó élek ill. pontok száma mind a négy esetben *legalább* annyi, mint a szóbanforgó utak száma, hisz a maximális számú út mindegyike egy-egy különböző élt ill. pontot tartalmaz a lefogókból. A továbbiakban tehát mind a négy esetben bebizonyítjuk, hogy a lefogó elemek száma *legfeljebb* annyi, mint a pont- ill. éldiszjunkt utak maximális száma.

1. Definiáljuk a $(G,u,v,\mathbf{1})$ hálózatot. Ebben a hálózatban minden uv egészfolyam 0-t vagy 1-t rendel minden élhez. Azon élek, melyekhez a folyam 1-t rendel, éldiszjunkt uv utaknak felelnek meg. A folyam értéke pedig éppen az iménti uv utak száma. Azt kaptuk, hogy a k értékű egészfolyamok kölcsönösen egyértelműen megfelelnek éldiszjunkt uv utak k-elemű halmazainak. Eszerint egy maximális egész folyam megad maximális számú éldiszjunkt uv utat. Az egészértékűségi lemma szerint a maximális folyam választható egészfolyamnak is, azaz a maximális egészfolyam értéke és a maximális folyam értéke azonos, konkrétan $\lambda_G(u,v)$. A Ford-Fulkerson tétel szerint tehát létezik a hálózatban egy $\lambda_G(u,v)$ kapacitású vágás. Ez a vágás éppen $\lambda_G(u,v)$ élt tartalmaz, amik a konstrukció miatt lefogják az összes uv utat.

2. Húzzunk szét minden u-tól és v-től különböző x pontot G-ben, azaz helyettesítsük x-t egy x_{be} és egy x_{ki} ponttal, vezessünk minden x-be futó élt egy, az x_{be} csúcsba érkező éllel, minden x-ből kiinduló élt egy, az x_{ki} csúcsból induló éllel, és húzzunk be egy $x_{be}x_{ki}$ élt is.

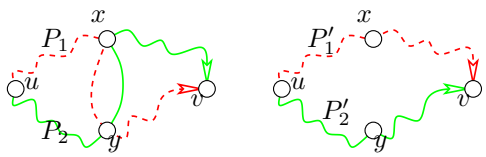


Ha ezt G minden $x \neq u, v$ csúcsára elvégezzük, akkor az így kapott G' gráfban k éldiszjunk uv út pontosan k pontdiszjunkt útnak felel meg G-ben, és viszont.

A már bebizonyított (első) Menger tétel szerint tehát létezik G'-nek $\kappa_G(u,v)$ éle, amik G' minden uv utját lefogják. Minden ilyen élnek kiválasztható egy-egy végpontja, aminek a G-beli megfelelője sem nem u, sem pedig v. (Itt használjuk ki, hogy u és v nem szomszédosak.) Világos, hogy ezáltal legfeljebb $\kappa_G(u,v)$ pontját jelöljük ki G-nek, ráadásul ezek a pontok a konstrukció folytán minden G-beli uv-utat lefognak.

3. Készítsük el a G' irányított gráfot úgy, hogy G minden élét oda és vissza is megirányítjuk! (G'-nek tehát kétszer annyi (hurokéltől különböző) éle lesz, mint G-nek.) Világos, hogy G'-ben létezik $\lambda_G(u,v)$ darab éldiszjunkt, irányított uv-út, hiszen G-ben van ennyi, és azok irányított változatai megteszik. Másfelől, ha G'-ben van k darab éldiszjunkt, irányított uv-út, akkor létezik k darab ilyen azzal a tulajdonsággal is, hogy ezen utak nem használnak ellentétesen irányított éleket.

Ha ugyanis egy $P_1 = (u \dots xy \dots v)$ út használja az xy élt, egy másik $P_2 = (u \dots yx \dots v)$ út pedig az yx élt, akkor a $P_1' = (u \dots x \dots v)$ illetve $P_2' = (u \dots y \dots v)$ utak ugyanazokat az éleket használják, mint P_1 és P_2, kivéve xy-t és yx-t.



Ha tehát minden olyan élre elvégezzük a fenti konstrukciót, melyet két út oda-vissza használ akkor G'-ben kapunk k darab *irányított* uv-utat, melyeknek a G-ben ugyanennyi (immár) éldiszjunkt, irányítatlan uv-út felel meg. Azt kaptuk tehát, hogy G'-ben az éldiszjunkt, irányított uv-utak maximális száma szintén $\lambda_G(u,v)$.

A már bizonyított első Menger tétel miatt létezik tehát G'-ben $\lambda_G(u,v)$ él, ami minden G'-beli uv-utat lefog. A konstrukció folytán ezen élek G-beli, irányítatlan megfelelői lefognak minden irányítatlan uv utat, ráadásul ez a G-beli élhalmaz is legfeljebb $\lambda_G(u,v)$ méretű.

4. Alkalmazzuk itt is a 3. rész bizonyításában használt konstrukciót: képezzük a G' gráfot a G éleinek oda-vissza irányításával. Világos, hogy az irányítatlan pontdiszjunkt G-beli uv-utak kölcsönösen egyértelműen megfelelnek az irányított, pontdiszjunkt G'-beli uv-utaknak. Tehát G'-ben az irányított pontdiszjunkt utak maximális száma $\kappa_G(uv)$. A már bizonyított, második Menger tétel alapján létezik G'-nek $\kappa_G(u,v)$ pontja, melyek minden irányított uv-utat lefognak. A konstrukció folytán ugyanezek a pontok lefognak G-ben is minden irányítatlan uv-utat, és nekünk éppen ezt kellett bizonyítanunk. □

A Menger tételek bizonyításának lényege, hogy kisebb-nagyobb átalakítások után az állítás közvetlenül adódik a hálózati folyamok MFMC tételéből, hiszen egy maximális diszjunkt útrendszer egy maximális *egész*folyamból, a minimális lefogó halmaz pedig egy minimális vágásból adódott. Ez a megfigyelés egy újabb előnyét mutatja a fenti bizonyításnak: amennyiben mi egy maximális pont- vagy éldiszjunkt útrendszerre illetve egy minimális, minden utat lefogó pont- vagy élhalmazra vagyunk kíváncsiak, akkor nem kell mást tenni, mint meghatározni az ismert módon egy maximális egészfolyamot illetve egy minimális vágást a gráfból képzett hálózatban.

Történelem Menger 1927-ben publikálta a tételét, amely eredeti formájában az irányítatlan pontdiszjunkt változattal volt ekvivalens. Kőnig Dénes észrevette, hogy a tétel Menger által adott bizonyítása hibás, és egyúttal ki is javította az eredeti bizonyítást: a hiányzó láncszem a páros gráfokra vonatkozó $\nu = \tau$ egyenlőség volt. Miután Kőnig levélben feltárta Mengernek a hibát, és elküldte neki, hogyan lehet kijavítani azt, Menger válaszában közölte, hogy tudott a dologról, és azt a készülő könyvében már kijavította. Azt, hogy hogyan, nem árulta el. Az említett könyvben valóban egy helyes bizonyítás szerepel, de Menger egy szóval sem közölte, hogy az eredeti bizonyítása hiányos volt, és Kőnig nevét is hiába keresnénk ennél a résznél.

Def: Az irányítatlan G gráfot *k-szorosan (pont)összefüggőnek* (röviden *k-összefüggőnek*) nevezzük, ha G-nek legalább $(k+1)$ pontja van, és G összefüggő marad, bárhogyan is hagyunk el belőle legfeljebb $k-1$ pontot. A maximális k-t, amire G k-összefüggő $\kappa(G)$ jelöli.

Def: A G irányítatlan gráfot *k-szorosan élösszefüggőnek* (röviden *k-élösszefüggőnek*) nevezzük, ha G összefüggő marad, bárhogyan is hagyunk el belőle legfeljebb $k-1$ élt. A maximális k-t, amire G k-élösszefüggő $\lambda(G)$ jelöli.

Tétel: Az irányítatlan G gráf pontosan akkor k-összefüggő ha G-nek legalább $(k+1)$ pontja van, és G bármely két, különböző pontja között létezik k pontidegen út. G pontosan akkor k-élösszefüggő, ha G bármely két, különböző pontja közt vezet k élidegen út.

Biz: Az irányítatlan Menger tételekből könnyen adódik: ha bármely két pont között van k út, akkor G nem eshet szét k-nál kevesebb pont ill. él elhagyásával. Ha G k-élöf, akkor semelyik két pont közti utakat sem fogja le k-nál kevesebb él (azok elhagyásával ugyanis G szétesne), ezért Menger 3. tétele szerint tetszőleges két pont között létezik k élidegen út. Ezzel a tétel éldiszjunkt változatát igazoltuk.

A pontdiszjunt esethez tegyük fel indirekt, hogy G k-öf, és u-ból v-be legfeljebb $k-1$ pontdiszjunk út

található. Ha u és v nem szomszédosak, akkor Menger 4. tétele miatt az uv-utak lefoghatóak legfeljebb $k-1$ ponttal. Ezek elhagyásával G szétesne, de ez ellentmond G k-szoros összefüggőségének.

Ha $uv \in E(G)$, akkor az uv él törlése után keletkező G' gráf legfeljebb $k-2$ pontdiszjunkt uv utat tartalmaz, tehát Menger 4. tétele szerint létezik $k-2$ pontja, aminek elhagyásakor G' szétesik. A szétesett gráfban ismét összekötve az u és v pontokat egy legalább 3-pontú gráfot kapunk (hisz G-nek legalább $k+1$ pontja volt), mely az uv élt törlésétől szétesik. De ekkor az uv él helyett u vagy v valamelyike is törölhető, hogy a gráf szétessen. Ismét azt kaptuk, hogy G legfeljebb $k-1$ alkalmas pont törlésével szétesik, ami a k-szoros összefüggőségnek mond ellent. □

Tétel: (Menger) Ha G legalább 3-pontú gráf akkor az alábbi állítások ekvivalensek.
(1) G 2-öf, (2) G bármely 2 pontján át vezet kör. Ha G-nek nincs izolált pontja, akkor a fentiekkel ekvivalens az is, hogy (3) G bármely 2 élén át vezet kör.

Biz: (1) $\Rightarrow$ (2). Ha G 2-öf, akkor bármely u, v pontja között van két pontidegen út, melyek együtt egy u-t és v-t tartalmazó kört alkotnak.
(2) $\Rightarrow$ (1). A kör tekinthető két pontidegen út uniójának, azaz bármely két pont között létezik legalább 2 pontidegen út, és az előző tétel szerint (figyelembevéve, hogy G legalább 3-pontú), azt jelenti, hogy G 2-öf.
(3) $\Rightarrow$ (2). Ha u-n és v-n keresztül akarunk kört találni, akkor elegendő egy-egy u-ra és v-re illeszkedő élen keresztül kört találni, ami a (3) feltétel szerint létezik.
(1) $\Rightarrow$ (3) G úgy is 2-öf marad, ha két élét felosztjuk egy-egy ponttal. (2) miatt létezik a felosztó pontokon keresztül kör, ami épp egy, a felosztott éleken keresztüli körnek felel meg. □

Dirac tétele: Ha G k-öf, és $k \geq 2$, akkor G bármely k pontján keresztül található kör G-ben. □

4. Páros gráfok és párosítások

Def: A G gráf *páros gráf*, ha csúcsai két színnel színezhetőek úgy, hogy G bármely élének végpontjai különböző színűek legyenek.

Megjegyzés: A fenti definícióban a két színnel való színezés nem feltétlenül egyértelmű: pl az n pontból álló üres gráf tetszőleges 2-színezése teljesíti a feltételt. (Könnyen látható, hogy pontosan akkor egyértelmű a két színnel való színezés, ha a páros gráf öf.) Egy rögzített 2-színezés esetén az azonos színűre színezett pontok halmazát *színosztálynak* nevezzük. A fenti definíció kimondható úgy is, hogy a páros gráf az, aminek a pontjai két osztályba sorolhatóak úgy, hogy élek kizárólag e két osztály között futhatnak.

Ha hangsúlyozni akarjuk, hogy a szóbanforgó G egy *páros* gráf, és egyúttal az A és B színosztályokat is meg szerenénk adni, akkor használhatjuk a $G = (A, B; E)$ jelölést.

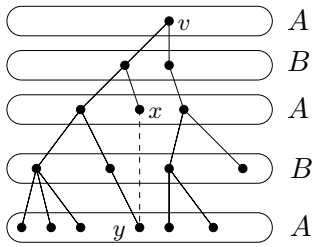
Megfigyelés: Minden páros hosszú kör páros gráf, t.i. felváltva ki lehet színezni a csúcsait. Páratlan körre ezt nem tehetjük meg, a páratlan kör tehát nem páros gráf. Ha egy gráf páros, akkor minden részgráfja is páros. Páros gráf ezért nem tartalmazhat ptn kört. Megadjuk a páros gráfok egy ekvivalens jellemzését.

Tétel: A G véges gráf pontosan akkor páros, ha G nem tartalmaz páratlan kört (azaz, ha G minden köre páros).

Köv.: Mivel a fában nincs kör (hát még ptn kör), ezért minden fa páros gráf.

A tétel bizonyítása: Szükségesség: az előző megfigyelésben láttuk be.

Elégségesség: tegyük fel, hogy G nem tartalmaz páratlan kört. Azt kell megmutatni, hogy létezik alkalmas 2-színezés. Mivel élek csak a gráf komponensein belül futnak, ezért elegendő egy komponensen belül találni egy 2-színezést, azaz feltehető, hogy G öf. Legyen F a G egy feszítőfája, és v pedig G egy tetszőleges pontja (F gyökere). Legyen A a v-től az F fán páros távolságra levő csúcsok, B pedig a v-től F-en páratlan hosszú úton elérhető csúcsok halmaza. Világos, hogy F minden éle A és B között fut, de megmutatjuk, hogy ugyanez G-re is igaz. Innen az állítás következik, hisz ezáltal G pontjait két színosztályra tudtuk bontani.



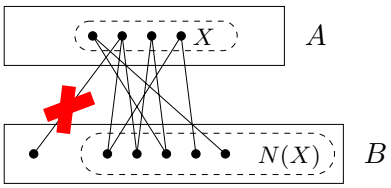
Ha tehát futna G-nek egy xy éle (mondjuk) az A halmazon belül (B-re a bizonyítás szó szerint megegyezik), akkor létezne G-ben egy $xy \ldots v \ldots x$ páratlan hosszúságú körséta, melyet az iménti él, a v-t az x-szel ill. a v-t az y-nal összekötő F-beli utak határoznak meg. Ha ebből a körsétából levágjuk az F-beli vx és vy utak közös részét, akkor a sétából páros sok él marad ki, és egy G-beli páratlan kört kapunk. Ellentmondás. □

Def: A $G = (V, E)$ gráf éleinek M részhalmaza *független*, más szóval M *(részleges) párosítás*, ha az M-beli élek végpontjai különbözőek, azaz G minden csúcsából legfeljebb egy M-beli él indul. Az M párosítás *teljes párosítás*, ha M G minden pontját *fedi*, azaz G minden csúcsára illeszkedik egy M-beli él.

Példa: Egy tánciskolában tanuló fiúk ill. lányok halmazai alkotssák a G páros gráf színosztályait. Fusson G-ben él két csúcs között, ha az adott fiú és lány hajlandóak egymással táncolni. Ekkor G minden párosítása egy lehetséges táncpartner-választási szituációt ír le. Ebben a modellben a hatékony oktatás érdekében a tánctanár minél több élből álló párosítást szeretne találni, mely optimális esetben egy teljes párosítás.

Egy másik lehetséges példa, ha a gráf csúcsai az egyetem termeinek ill. az ott folyó előadásoknak felelnek meg. Akkor van él egy teremnek és egy előadásnak megfelelő csúcs között, ha a terem alkalmas az adott előadás megtartására. Egy adott pillanatban az egyetemen folyó tevékenység egy párosítást indukál az előbb definiált segédgráfban.

Def: A $G = (V, E)$ gráf $X \subseteq V$ ponthalmaz szomszédainak halmazát $N(X)$ jelöli: $N(X) := \{v \in V : \exists x \in X, \text{melyre } xv \in E\}$.



Frobenius tétele: A $G = (A, B; E)$ véges, páros gráfnak pontosan akkor létezik teljes párosítása, ha $|A| = |B|$ és $|X| \leq |N(X)|$ minden $X \subseteq A$ ponthalmazra.

Hall tétele: A $G = (A, B; E)$ véges, páros gráfnak pontosan akkor létezik A-t fedő párosítása, ha $|X| \leq |N(X)|$ minden $X \subseteq A$ ponthalmazra.

A Frobenius tétel triviálisan következik a Hall tételből, így elég ez utóbbit igazolni. A Hall tételt pedig a Kőnig tétel speciális eseteként fogjuk belátni.

Def: Adott G gráf esetén $\nu(G)$ jelöli a G független élhalmazai közül a maximális méretét, azaz G maximális párosításának elemszámát.

Def: A G gráf pontjainak U halmaza *lefogó ponthalmaz*, ha G minden élének van U-beli végpontja. A legkevesebb pontból álló lefogó ponthalmaz méretét $\tau(G)$ jelöli.

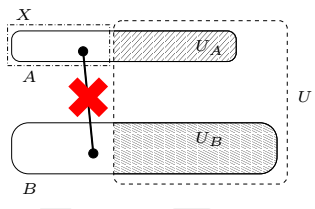
Állítás: Ha G véges gráf, akkor $\nu(G) \leq \tau(G)$. (G nem feltétlenül páros gráf.)

Biz: Legyen M G-nek egy maximális ($\nu(G)$ élből álló) párosítása. Ha U egy minimális méretű lefogó ponthalmaz, akkor lefogja M minden élét is, ám U minden pontja legfeljebb egy párosításélt fog le. Tehát $\tau(G) = |U| \geq |M| = \nu(G)$. □

Kőnig tétele: Ha $G = (A, B; E)$ véges, páros gráf, akkor $\nu(G) = \tau(G)$.

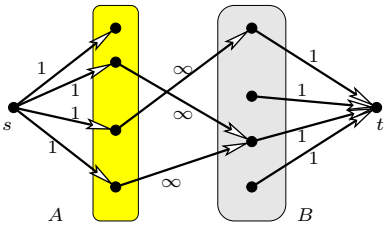
A Hall tétel bizonyítása: A szükségesség nyilvánvaló: ha létezik A-t fedő párosítás, akkor minden A-beli pontnak különböző párja van, tehát tetszőleges $X \subseteq A$ esetén az X-beli elemek B-beli párjai az $N(X)$ egy $|X|$ méretű részhalmazát alkotják.

Az elégségességhez tegyük fel, hogy $|X| \leq |N(X)|$ minden $X \subseteq A$-ra. Azt kell igazolnunk, hogy $\nu(G) \geq |A|$. Legyen U minimális (azaz $\tau(G)$ méretű) lefogó ponthalmaz, és legyen $U_A := U \cap A$, $U_B := U \cap B$. Mivel U lefogja az $X := A \setminus U_A$-ból induló éleket, ezért $N(X) \subseteq U_B$, tehát $|N(X)| \leq |U_B|$. A Kőnig tétel ill. Hall a feltétel miatt



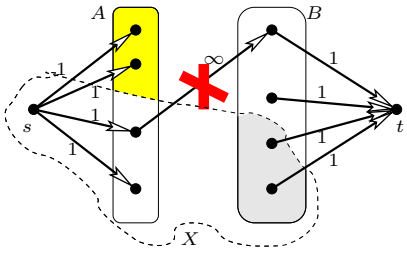
$$\nu(G) = \tau(G) = |U| = |U_A| + |U_B| \geq |U_A| + |N(X)| \geq |U_A| + |X| = |A| \ .\square$$

A Kőnig tétel bizonyítása: Készítsünk el a G' gráfot az alábbiak szerint. Irányítsuk G minden élét A-ból B-be, vegyünk fel egy új s és t pontot, vezessünk s-ből élt A minden pontjába, és vegyünk fel egy-egy élt B minden pontjából t-be. Adjunk minden élnek kapacitásokat: az s-ből induló ill. t-be érkező éleké legyen 1, az A-ból B-be futóké pedig legyen ∞ (pontosabban $|A|+1$). Tekintsük a (G', s, t, c) hálózatot, ahol c az imént definiált kapacitást jelenti.



Vegyük észre, hogy ha G-ben van egy k méretű párosítás, akkor létezik ebben a hálózatban k értékű egészfolyam: a párosításéleknek megfelelő éleken, az ezen élek A-beli végpontjaihoz vezető s-ből induló éleken, valamint a párosításélek B-beli végpontjaiból t-be vezető éleken legyen a folyam által felvett érték 1, minden egyéb élen 0. Az is könnyen látható, hogy a hálózatban minden egészfolyam úgy áll elő, hogy néhány, A-ból B-be vezető független élen a folyam 1 értéket vesz fel, ezeket az éleket s-ből tápláljuk, a kifolyó folyamot pedig t-be engedjük. A hálózatban tehát a maximális egészfolyam értéke $\nu(G)$, és az egészértékűségi lemma miatt a maximális folyamérték is ugyanennyi.

A Ford-Fulkerson tétel szerint létezik tehát egy $\nu(G)$ értékű vágás. Ha ezt a vágást az s-t tartalmazó X halmaz definiálja, akkor $X \cap A$-ból nem futhat G'-nek éle $B \setminus X$-be, hisz akkor a vágás kapacitása ∞ volna. (Pontosabban legalább $|A|+1$, de már az is több, mint $\nu(G)$, hisz A egy lefogó halmaz, ahonnan $\nu(G) \leq |A|$.) Ez azt jelenti, hogy $(A \setminus X) \cup (B \cap X)$ egy lefogó ponthalmaz, tehát $|A \setminus X| + |B \cap X| \geq \tau(G)$. A hálózat konstrukciójából adódóan az X által definiált vágás kapacitása $\nu(G) = |A \setminus X| + |B \cap X| \geq \tau(G)$. A Kőnig tétel előtt bizonyítottuk, hogy $\nu(G) \leq \tau(G)$ áll, ahonnan $\nu(G) = \tau(G)$ adódik. □



A fenti bizonyításból hatékony algoritmust kapható egy maximális párosítás ill. egy minimális lefogó ponthalmaz megtalálására páros gráfban. Ha a maximális folyamok meghatározására szolgáló javító utas módszert a fenti konstrukcióra alkalmazzuk, és eltekintünk az s-re ill. t-re illeszkedő élektől, akkor a következő eljárást[7] kapjuk. Kiindulunk az üres párosításból, és azt javítgatjuk. Ha már találtunk egy M párosítást, akkor tekintjük az M-hez tartozó segédgráfot, azaz M éleit B-ből A-ba irányítjuk, G egyéb éleit pedig A-ból B-be. Ha ebben a segédgráfban létezik egy P irányított út egy A-beli, az aktuális M párosítás által fedetlen pontból olyan B-beli pontba, melyet szintén nem fed a párosítás, akkor ezen az ú.n. *alternáló úton* az eddigi párosításéleket elhagyva, és P párosításon kívüli éleit bevéve (más szóval M helyett $M \Delta P$ tekintve), egy eggyel nagyobb méretű párosítást kapunk. Ha pedig nincs javító alternáló út, akkor M maximális párosítás, és könnyen található egy $|M|$ csúcsot tartalmazó lefogó ponthalmaz is.

A Kőnig tétel levezethető Menger tételéből is. Annak oka, hogy nem így jártunk el, az volt, hogy a maximális párosítást kereső algoritmus, mint a maximális folyamkeresés speciális esete jobban látszik a közvetlen visszavezetésből. Érdemes azonban látni e két tétel kapcsolatát is, ezért az alábbiakban közöljük ezt a bizonyítást is. (És igen: a vizsgán ezt is elfogadjuk az elsőnek közölt bizonyítás helyett.)

A Kőnig tétel második bizonyítása: Most hagyjuk meg a G gráfot irányítatlannak, de vegyük fel az s és t pontokat, vezessünk s és A minden pontja ill. t és B minden pontja között egy-egy élt. Világos, hogy ha létezik G-ben k független él, akkor ezek segítségével találunk k pontdiszjunkt st-utat a fent konstruált G' gráfban. Másfelől, ha ismerünk k pontdiszjunkt st-utat G'-ben, akkor az ezek által használt G-beli élek függetlenek. Tehát a G-ben a független élek maximális száma megegyezik G'-ben a pontdiszjunkt st-utak maximális számával: $\nu(G) = \kappa_{G'}(s,t)$.

Minthogy G'-ben s és t nem szomszédosak, alkalmazhatjuk Menger 4. tételét, amely szerint a pontdiszjunt st-utak maximális száma ($\kappa_{G'}(s,t)$) megegyezik a minden st-utat lefogó, s-től és t-től különböző pontok minimális számával. Csupán azt kell észrevenni, hogy G csúcsainak egy U részhalmaza pontosan akkor fogja le G minden élét, ha ugyanez az U ponthalmaz G'-ben lefog minden st-utat. Tehát G-ben a lefogó pontok minimális száma megegyezik a G'-ben minden st-utat lefogó, s-től és t-től különböző pontok minimális számával: $\tau(G) = \kappa_{G'}(s,t) = \nu(G)$, ahol az utóbbi egyenlőséget a bizonyítás első részében láttuk be. □

Történelem Frobenius 1912-ben publikált egy determinánsokra vonatkozó eredményt, ami a gráfok nyelvén fogalmazva a páros gráfok teljes párosításának jellemzésével egyenértékű. Kőnig ettől az eredménytől függetlenül találta meg a fent ismertetett Kőnig tételt 1915-ben, amit aztán elküldött Frobeniusnak. Frobenius később megjelentetett egy elemi bizonyítást a tételére, és megemlítette Kőniget is, mint akinek a tétele könnyen következik az övéből. Mindezen túl megjegyezte azt is, hogy az a gráfelmélet masinéria, amin Kőnig bizonyítása alapszik nem sokat segít a determinánsok elméletében, hiszen Kőnig tétele egy meglehetősen speciális, nem sokat érő állítás. Minden, ami Kőnig eredményéből használható, benne van Frobenius determinánsokról szóló tételében.

Nos, az idő nem Frobeniust igazolta.

Def: A G gráf pontjainak U részhalmaza *független* (vagy *stabil*), ha U nem feszít élt, azaz G minden élének van nem U-beli végpontja. A G gráf legtöbb pontból álló, független ponthalmazának méretét $\alpha(G)$ jelöli.

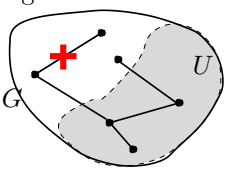
Def: A G gráf éleinek F halmaza *lefogó élhalmaz*, ha G minden pontjából indul F-beli él. A G gráf legkevesebb élből álló, lefogó élhalmazának méretét $\rho(G)$ jelöli.

Megfigyelés: Tetszőleges, véges G gráfra $\alpha(G) \leq \rho(G)$.

Biz: Egy $\alpha(G)$ méretű független ponthalmaz lefogásához legalább $\alpha(G)$ él szükséges. □

Gallai tétele: Legyen G n-pontú gráf.

1. Ha G-ben nincs hurokél, akkor $\tau(G) + \alpha(G) = n$.
2. Ha G-nek nincs izolált pontja, akkor $\nu(G) + \rho(G) = n$.



Biz: 1.: Könnyen látható, hogy $U \subseteq V(G)$ pontosan akkor lefogó ponthalmaz, ha $V(G) \setminus U$ független ponthalmaz. Az állítás innen közvetlenül adódik.

[7] Néha –kissé helytelenül– az ismertetett eljárást *magyar módszernek* nevezik. A magyar módszer az amerikai Harold Kuhn találmánya. Történt ugyanis 1953-ban, hogy Kuhn éppen Kőnig Dénes könyvét lapozgatta, amikoris megakadt a szeme egy lábjegyzeten, mely Egerváry Jenő egy 1931-ből származó magyar nyelvű cikkére hivatkozik, mint a maximális párosításokról szóló $\nu = \tau$ tétel általánosítására. Kuhnt pedig éppen az a probléma érdekelte, hogy hogyan lehet egy páros gráfban nem maximális, hanem *maximális súlyú* párosítást találni. (A maximális párosítás a maximális súlyúnak speciális esete, amennyiben minden él súlya pontosan 1.) Nos, a nyom helyesnek bizonyult: Egerváry cikkében valóban erről volt szó. Ám ahhoz, hogy ez kiderüljön, egy kis elszántságra volt szükség: Kuhn egy magyar szótár és egy nyelvtankönyv segítségével két hét alatt lefordította magának a cikket. A módszer segítségével, a cikkben leírtak szerint meghatározott egy maximális súlyú párosítást egy háromjegyű élsúlyokkal rendelkező, 24 csúcsú páros gráfban. Ehhez mindössze 3 órára volt szüksége, ami meggyőzte őt a módszer helyességéről. Magát az algoritmust tehát Kuhn írta le, de Egerváry tiszteletére magyar módszernek nevezte el, és azóta az egész világ így ismeri.

2.: Mivel G-nek létezik $\nu(G)$ diszjunkt éle, ezek $2\nu(G)$ pontot fognak le. A maradék $n-2\nu(G)$ pont mindegyike lefogható egy-egy új éllel (hisz nincs izolált pont), azaz $\nu(G)+n-2\nu(G)=n-\nu(G)$ éllel minden pont lefogható. Innen $\rho(G)\le n-\nu(G)$, ahonnan $\nu(G)+\rho(G)\le n$ adódik.

Másrészről, könnyen látható, hogy ha F minimális méretű lefogó élhalmaz, akkor F körmentes, és nem tartalmaz 3 hosszú utat sem. Tehát F diszjunkt csillagok uniója. (A csillag olyan öf gráf, melynek (legfeljebb) egy híján minden pontjának foka 1.) Ha a minimális lefogó élhalmazban k csillag van, akkor e halmaz $n-k$ élt tartalmaz, másrészt e halmaz tartalmaz k diszjunkt élt, tehát $\nu(G)\ge k$. Azt kaptuk, hogy $\rho(G)+\nu(G)\ge n-k+k=n$, és innen a másik irányú egyenlőtlenség figyelembevételével következik a tétel. □

A Gallai tétel egy lehetséges alkalmazása a

Kőnig tétel. Ha a G véges, páros gráfnak nincs izolált pontja, akkor $\alpha(G)=\rho(G)$

Biz: Páros gráfban hurokél nem lehet, így az állítás következik Kőnig előző tételéből és Gallai két tételéből: $\alpha(G)=|V(G)|-\tau(G)=|V(G)|-\nu(G)=\rho(G)$. □

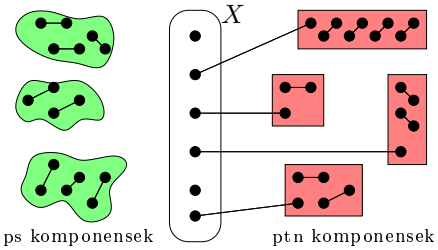
A maximális párosítás méretének (azaz a $\nu(G)$ gráfparaméternek) a meghatározása nem csak páros gráfok esetén érdekes. Ezért hasznos megfigyelés, hogy a javító alternáló utakkal való növelés (elméletileg) itt is maximális párosítást ad. (A páros gráfokon használt alternáló ill. javító út fogalma értelemszerűen kiterjed nem páros gráfokra is.)

Berge tétele: A G gráf M párosítása pontosan akkor maximális, ha nincs M-hez javító út.

Biz: Ha M nem maximális, akkor létezik egy $|M|$-nél több élt tartalmazó N párosítás. Az $M\cup N$ élhalmaz egy komponense vagy a két párosítás közös éle, vagy egy olyan M-alternáló út, mely egyben N-alternáló is egyúttal (ún. MN-alternáló út), vagy egy olyan kör, melynek élei felváltva M ill. N-beliek (MN-alternáló kör). Mivel $|N|>|M|$, ezért kell olyan MN-alternáló útnak lennie, ami több N-beli élt tartalmaz, mint M-belit. Az ilyen út az M párosítás javító útja. □

Hogyan lehet bebizonyítani, hogy egy adott gráf nem tartalmaz teljes párosítást? Páros gráf esetén láttuk, hogy egy színosztályméretnél kisebb lefogó ponthalmaz megfelelő bizonyíték. Jó ez a bizonyíték nem páros gráfokra is, de pl. már K_3 esetén sem elég jó: $\nu(K_3)=1<2=\tau(K_3)$. Nem páros esetre a következő állítás mutat egy lehetséges bizonyítékot. Egy G gráf páratlan komponenseinek számát $c_p(G)$ jelöli.

Állítás: Ha a G véges gráfnak létezik k olyan pontja, melyek elhagyása után több, mint k páratlan komponens keletkezik (azaz $c_p(G-X)>|X|$ valamely $X\subseteq V(G)$-re), akkor G-nek nincs teljes párosítása.



Biz: Ha G-nek van teljes párosítása és $X\subseteq V(G)$, akkor $G-X$ minden páratlan komponensének van olyan v pontja, hogy a v-t fedő párosításél nem a komponensen belül fut, azaz kilép a belőle. Ezen párosításél másik végpontja szükségképp X-ben van. Tehát minden páratlan komponenshez tartozik egy-egy különböző X-beli pont. □

A fenti állítás alkalmas megfordítása is igaz.

Tutte tétele: A véges G gráfnak pontosan akkor van teljes párosítása, ha tetszőleges $X\subseteq V(G)$ esetén $c_p(G-X)\le|X|$ teljseül. □

5. Gráfok színezései

Def: A G gráf *k színnel színezhető*, ha G minden csúcsa kiszínezhető k adott szín valamelyikére úgy, hogy G minden élének mindkét végpontja különböző színű legyen. A G gráf *kromatikus száma* $\chi(G)=k$, ha G kiszínezhető k színnel, de $k-1$ színnel még nem. Más szavakkal, $\chi(G)$ a legkisebb olyan k egész, melyre G csúcsai lefedhetőek k független ponthalmazzal.

Megjegyzés: 1. Ha G k-színezhető, akkor G-ben nincs hurokél.
2. A G gráf k-színezése tkp. egy $c:V(G)\to\{1,2,\dots,k\}$ fv, melyre $c(u)=c(v)\Rightarrow uv\notin E(G)$ áll.

Példa: 1. G pontosan akkor páros gráf, ha $\chi(G)\le 2$. (T.i. G 2-színezése úgy bontja két részre a csúcshalmazt, hogy él csak a színosztályok közt futhat, és viszont.)
2. Páratlan n-re C_n nem páros gráf, így $\chi(C_n)\ge 3$. Mivel C_n 3-színezhető, ezért $\chi(C_n)=3$.

Def: A G gráf *klikkje* a G teljes részgráfja. A G gráf $\omega(G)$-vel jelölt *klikkszáma* G legnagyobb klikkjének pontszáma, azaz a legnagyobb olyan k szám, melyre létezik G-ben k páronként összekötött csúcs, de $k+1$ már nem létezik.

Állítás: Minden irányítatlan, véges G gráfra $\omega(G)\le\chi(G)\le\Delta(G)+1$.

Biz: G pontjainak kiszínezésével a maximális klikk pontjait is kiszínezzük, mégpedig különböző színekkel. Ebből világos az első egyenlőtlenség.

Másrészt az alábbi mohó algoritmus segítségével bármely G gráf $(\Delta(G)+1)$-színezhető. Színezzük ki G pontjait $v_1, v_2, \ldots v_n$ sorrendben úgy, hogy az i-dik lépésben v_i-t olyan színre színezzük, ami nem szerepel v_i kiszínezett szomszédain. Mivel v_i-nek legfeljebb $\Delta(G)$ kiszínezett szomszédja lehet, és mindegyik szomszéd legfeljebb egy-egy színt zár ki, v_i színezése elvégezhető a rendelkezésre álló színek valamelyikével. v_n kiszínezése után G egy $(\Delta(G)+1)$-színezését kapjuk, ami a második egyenlőtlenséget igazolja. □

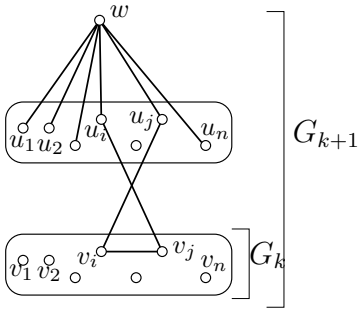
Megjegyzés: A fenti állításban egyik egyenlőtlenséget sem lehet *általában* megjavítani: az alsó becslés pl. a később vizsgált perfekt gráfokra éles, míg a felső becslés teljes gráfokra és ptn körökre is pontos: $\chi(K_n) = n = \Delta(K_n)+1$ ill. $\chi(C_{2n+1}) = 3 = \Delta(C_{2n+1})+1$. A felső becslés azonban lényegében csak az utóbbi gráfokra éles.

Brooks tétele: Legyen G véges, egyszerű, öf gráf. Ha G nem teljes gráf és nem páratlan kör, akkor $\chi(G) \leq \Delta(G)$. □

Az alábbi tétel azt mutatja, hogy az $\omega(G) \leq \chi(G)$ alsó becslés sokszor bizony fabatkát sem ér.

Tétel: Tetszőleges $k \geq 2$ pozitív egészhez létezik olyan G gráf, melyre $\chi(G) = k$ és $\omega(G) = 2$.

Biz: Megadunk egy G_k gráfot a kívánt tulajdonsággal. A konstrukció egyébként Mycielski nevéhez fűződik. A k paraméter szerinti indukcióval bizonyítunk. A $G_2 = K_2$ megfelelő gráf, tehát $k = 2$-re az indukciós állítás igaz. Tegyük fel, hogy a G_k gráfot már sikerült elkészíteni. Legyen $V(G_k) = \{v_1, v_2, \ldots, v_n\}$, és $V(G_{k+1}) = \{v_1, v_2, \ldots, v_n\} \cup \{u_1, u_2, \ldots, u_n\} \cup \{w\}$, ahol az u_i és w az eddigiektől és egymástól különböző új csúcsok. Legyen $E(G_{k+1}) := \{wu_i : 1 \leq i \leq n\} \cup \{v_iu_j, v_ju_i : v_iv_j \in E(G_k)\} \cup E(G_k)$, azaz kössük össze w-t minden u_i-vel, továbbá minden G_k-beli él (önmagán kívül) két élért felelős G_{k+1}-ben.



Mivel az u_i pontok függetlenek, továbbá w-ből nem fut él v_i-be, ezért G_{k+1}-ben minden háromszög legalább két G_k-beli pontot (mondjuk v_i-t és v_j-t) tartalmaz. Ha a harmadik pontja egy u_l, akkor v_i, v_j, v_l a G_k-ban háromszöget alkotnak, ami ellentmond az indukciós feltevésnek. Azaz $\omega(G_{k+1}) = 2$. Azt kell már csak bebizonyítani, hogy G_{k+1} $(k+1)$-kromatikus. k szerinti indukciót használunk: $k = 2$-re $\chi(K_2) = 2$ miatt az állítás igaz. Világos, hogy $\chi(G_{k+1}) \leq k+1$, hisz a v_i-ket a G_k egy k-színezése szerint színezve, minden u_i-nek a v_i-vel azonos színt adva és w-re egy $(k+1)$-dik színt használva G_{k+1} egy $(k+1)$-színezését kapjuk.

Azt kell megmutatnunk, hogy G_{k+1} nem színezhető ki k színnel. Indirekt bizonyítunk: tegyük fel, hogy G_{k+1} mégis kiszínezhető k színnel. Tekintsünk egy ilyen színezést, és színezzük át a w-vel azonos színt kapó v_i pontokat u_i színére. Ezáltal a $\{v_1, v_2, \ldots, v_n\}$ pontok mindegyike w-étől különböző színt kap. Tehát G_k pontjait $(k-1)$-színeztük. Mivel $\chi(G_k)$ nem színezhető jól $k-1$ színnel, ezért az iménti színezésben lesz két azonos színt kapó, szomszédos csúcs, mondjuk v_i és v_j. Ezek az eredeti színezésben természetesen különböző színt kaptak, tehát az egyikük (mondjuk v_i) a w-vel azonos színt kapott, és ezért átszíneztük u_i színére. Azonban v_j és u_i is szomszédosak G_{k+1}-ben, tehát eredeti színük különböző volt. Ezért az átszínezés után sem fordulhat elő, hogy v_i és v_j azonos színt kapott. Ez az ellentmondás igazolja az indukciós állítást, azaz $\chi(G_{k+1}) = k+1$. □

Láttuk, hogy a 2-színezhető gráfok pontosan a páros gráfok. A 3-színezhető gráfok már sokkal bonyolultabb struktúrát alkotnak: annak a felismerése, hogy egy adott G gráf 3-színezhető-e (azaz G csúcsai előállnak-e 3 független ponthalmaz uniójaként), bizonyíthatóan nehéz. Figyelemreméltó, hogy a 4-színezhető gráfok osztálya tartalmazza a síkbarajzolható gráfokat.

4-szín tétel: Minden egyszerű, síkbarajzolható gráf 4-színezhető. □

Történelem Síkbarajzolt gráfok színezése legtermészetesebben a térképszínezés kapcsán merül fel: egy politikai térképen szeretnénk az országokat úgy kiszínezni, hogy szomszédos országok színe különbözzék[8]. Más szóval, egy síkbarajzolt gráf tartományait kell színeznünk, ami ekvivalens az adott gráf duálisának színezésével.

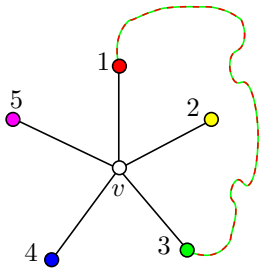
A 4-szín tételt Francis Guthrie sejtette először 1852-ben, midőn megfigyelte, hogy Anglia megyéi a 4-színezhetőek. Többszörös áttétellel értesült erről Cayley, aki 1878-ban publikálta a sejtést. 1879-ben Kempe közölt egy bizonyítást, melyet Tait bizonyítása követett 1880-ban. 1890-ben Heawood hibát talált Kempe bizonyításában, 1891-ben pedig Petersen a Tait-félében. A hibákat azóta sem sikerült kijavítani. Sokak hosszú, eredménytelen próbálkozásai után Appel és Haken 1976-ban bizonyították be a tételt. Módszerükkel az állítás egy hihetetlenül bonyolult, szerteágazó esetvizsgálatra vezetett, amit számítógéppel végeztek el. Mivel a bizonyítás helyességének ellenőrzése elképzelhetetlen számítógép nélkül, felmerült az a metamatematikai probléma, hogy mi tekinthető teljes értékű bizonyításnak: mennyire lehetünk biztosak abban, hogy a számítógépprogram valóban azt végzi el, amit arról feltételezünk. A történet jelenlegi utolsó állomásához 1996-ban érkezett, amikoris Robertson, Sanders, Seymour és Thomas talált egy, az Appel-Haken-félénél jóval egyszerűbb bizonyítást, mely

[8]Ez sem egészen igaz, ugyanis a politikai térképek nem szükségképpen 4-színezhetőek, hisz pl. Kalinyingrádot is az Oroszországhoz használt színnel kell festeni. Ha ezt jól megértettük, akkor nem meglepő az az állítás sem, hogy tetszőleges k-hoz létezik olyan politikai térkép, ami nem színezhető ki k színnel.

arra vezet, hogy 633 kis gráf 4-színezhetőségét kell ellenőrizni. Természetesen ezt is számítógéppel végezték, de a bizonyítás helyessége immár „kézzel" is ellenőrizhető. Persze enek közlése is meghaladja a jegyzet kereteit. Kempe módszere viszont alkalmas egy gyengébb, ám nemtriviális eredmény igazolására.

5-szín tétel: Minden egyszerű, síkbarajzolható G gráf 5-színezhető, azaz $\chi(G) \leq 5$.

Biz: Legfeljebb 3-pontú gráfokra a tétel triviálisan igaz. Pontszám szerinti indukcióval bizonyítunk, tegyük fel, hogy a legfeljebb $(n-1)$-pontú gráfokra a tétel igaz. Legyen G egy n-pontú ($n > 3$), egyszerű, síkbarajzolható gráf. Tudjuk, hogy G élszáma legfeljebb $3n-6$, azaz G pontjainak fokszámösszege legfeljebb $6n-12$. Van tehát G-nek egy legfeljebb 5-ödfokú v csúcsa.

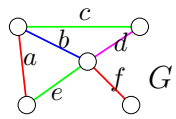


Mivel $G-v$ is egyszerű és síkbarajzolható, ezért az indukciós feltevés miatt 5-színezhető. Ha tehát v szomszédai legfeljebb 4 színt kapnak e színezésben, akkor v megkaphatja az ötödik színt. Ez akkor nem működik, ha $d(v) = 5$ és mind az öt szomszéd különböző színű[9]. (Ld. az ábrát.) Tekintsük az 1-es és 3-as színek által feszített G_{13} részgráfot $(G-v)$-ben. Ha a v csúcs 1-es ill. 3-as színű szomszédai G_{13} különböző komponenseibe esnek, akkor pl. az 1-es szomszéd komponensében felcserélve az 1-es és 3-as színeket, a $G-v$ olyan 5-színezését kapjuk, melyben v-nek nincs 1-es színű szomszédja. Ekkor v 1-es színre színezhető.

Ellenkező esetben van v 1-es és 3-as színű szomszédja között egy olyan út, mely csak 1-es és 3-as színű csúcsokat használ. A síkbrarajzoltság miatt biztos nincs v 2-es és 4-es színű szomszédja között olyan út $(G-v)$-ben, ami csak 2-es és 4-es színű csúcsokat használ, vagyis a G_{13}-hoz hasonlóan definiált G_{24} gráfban az említett két szomszéd különböző komponensekben van. A 2-es színű szomszéd komponensében felcserélve a 2-es és 4-es színt $G-v$ olyan 5-színezését kapjuk, amelyben v szomszédai között nem fordul elő a 2-es szín. A v csúcs tehát megkaphatja a 2-es színt. □

Megjegyzés: Érdemes meggondolni, hogy a fenti bizonyítás miért nem működik 4 színre.

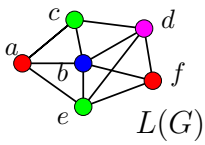
Def: A G gráf *élgráfja* az az $L(G)$ gráf, aminek a csúcsai G éleinek felelnek meg, és $L(G)$ két csúcsa pontosan akkor van éllel összekötve, ha G megfelelő élei szomszédosak.



Def: A G gráf *k-élszínezhető*, ha G élei k színnel színezhetőek úgy, hogy szomszédos élek különböző színt kapnak. A G gráf $\chi'(G)$ *élkromatikus száma* k, ha G k-élszínezhető, de G nem $(k-1)$-élszínezhető.

Megjegyzés: G pontosan akkor k-élszínezhető, ha $L(G)$ k-színezhető, továbbá $\chi'(G) = \chi(L(G))$.

Állítás: Tetszőleges G gráfra $\omega(L(G)) \geq \Delta(G)$, továbbá, ha $\Delta(G) \geq 3$, akkor $\omega(L(G)) = \Delta(G)$.



Biz: Az egy csúcsból induló éleknek megfelelő pontok klikket alkotnak $L(G)$-ben. Másfelől $L(G)$ minden klikkje vagy G egy csúcsból induló néhány élének, vagy G egy háromszögének felel meg. □

Állítás: Tetszőleges G gráfra $\chi'(G) \geq \Delta(G)$ áll.

Biz: Az egy csúcsból induló élek egymástól különböző színt kapnak, és ez speciálisan a maximális fokszámú csúcsból induló élekre is igaz. Ugyanez formálisan: $\chi'(G) = \chi(L(G)) \geq \omega(L(G)) \geq \Delta(G)$. □

Kőnig tétel: Ha $G = (A, B; E)$ páros gráf, akkor $\chi'(G) = \Delta(G)$.

Biz: Az előző állítás miatt elegendő azt igazolni, hogy $\chi'(G) \leq \Delta(G)$, azaz csupán egy $\Delta(G)$-élszínezést kell mutatni. Létezik olyan H páros gráf, melynek G részgráfja, és G' minden csúcsának fokszáma $\Delta(G)$. (Ilyen H-t például úgy kaphatunk, hogy G mellé felvesszük még G-nek egy $G' = (A', B'; E')$ másolatát, H színosztályai $A \cup B'$ és $B \cup A'$ lesznek, és minden v csúcsot összekötünk $\Delta(G) - d(v)$ párhuzamos éllel a v' másolatával.) Ha sikerül a $\Delta(G)$-reguláris H gráf éleit $\Delta(G)$ színnel kiszínezni, akkor egyúttal a G részgráf éleinek is megkapjuk egy ugyanennyi színnel való színezését.

A H gráf élszínezéséhez pedig elegendő azt megmutatni, hogy tetszőleges reguláris páros gráfban van teljes párosítás. Ugyanis akkor H egy teljes párosítását kiszínezve az első színnel, a színezetlen élek egy $(\Delta(G)-1)$-reguláris páros gráfot alkotnak, abban is találunk teljes párosítást, ez a második színt kapja, sít.

Miért létezik tehát egy r-reguláris páros gráfnak teljes párosítása? A Hall feltétel teljesülését kell csupán ellenőrizni. Ha az egyik színosztályból kiválasztunk egy k pontú X halmazt, akkor az X-beli csúcsokból összesen kr él indul ki. Mindezen élekből a másik színosztály bármely csúcsa legfeljebb r-t fogadhat be, tehát a kr darab él megérkezéséhez legalább k pontra van szükség: $|N(X)| \geq |X|$. A Hall feltétel az r-reguláris gráf bármelyik színosztályára teljesül, tehát csakugyan létezik teljes párosítás, és pontosan ezt kellett bizonyítanunk. □

Míg a $\chi \geq \omega$ becslés általában nem túl jó (mutatják ezt a Mycielski gráfok), addig a fenti becslés közel jár az igazsághoz.

Vizing tétele: Ha G véges, egyszerű gráf, akkor $\chi'(G) \leq \Delta(G) + 1$. □

[9] Ha csak a 6-színtételt szeretnénk igazolni, akkor ez sem okozna problémát, és a bizonyítást itt be is fejezhetnénk.

6. Perfekt gráfok

Az idei előadáson jóval kevesebbet mondtunk el perfekt gráfokról, mint amennyit egyébként szoktunk. Az elhagyott anyagot az apró betűs részek tartalmazzák, ezeket (idén) nem kell tudni a vizsgán.

Def: A G véges gráf *perfekt*, ha G minden feszített G' részgráfjára $\chi(G') = \omega(G')$ teljesül.

Megjegyzés: A fenti definíciót az motiválja, hogy azoknak a gráfoknak a szerkezetére vagyunk kíváncsiak, amelyekre a kromatikus számra vonatkozó, $\chi(G) \geq \omega(G)$ alsó becslés egyenlőséggel teljesül. Ebben a formában a kérdés nem szerencsés, mert tetszőleges (véges) G gráfhoz egy $\chi(G)$ méretű klikk-komponenst hozzávéve $\chi(G) = \omega(G)$ fog teljesülni. Ezért kívánjuk meg az egyenlőséget minden feszített részgráfra.

Példa: Ha G nemüres, páros gráf, akkor $\chi(G) = 2 = \omega(G)$ (üres páros gráfra $\chi(G) = \omega(G) = 1$). Mivel páros gráf feszített részgráfja is páros gráf, ezért minden páros gráf perfekt.
Minden út páros gráf, ezért minden út perfekt.
$\chi(K_n) = n = \omega(K_n)$, továbbá minden klikk feszített részgráfja klikk, ezért minden klikk perfekt.
Ha $n \geq 2$, akkor $\chi(C_{2n+1}) = 3 \neq 2 = \omega(C_{2n+1})$, tehát a páratlan kör (a $C_3 = K_3$ kivételével) nem perfekt gráf. (Viszont minden feszített részgráfja perfekt, tehát a legalább 5 hosszú ptn kör egy *minimális imperfekt gráf.*)

Az alábbi tételek további gráfosztályok perfektségét igazolják:

Tétel: Ha G komplementere páros gráf, akkor G perfekt.

Biz: Ha G páros gráf komplementere, akkor G minden feszített részgráfja is páros gráf komplementere, ezért elegendő azt bizonyítani, hogy $\chi(G) = \omega(G)$ ha G komplementere páros. Kőnig és Gallai tételei alapján (páros gráfban nincs hurokél) $\omega(G) = \alpha(\overline{G}) = n - \tau(\overline{G}) = n - \nu(\overline{G})$. Az egyenlőség igazolásához elegendő a $\chi(G) \leq \omega(G)$ bizonyítása, azaz G egy $n - \nu(\overline{G})$ színnel történő színezésének megadása. Ilyet pedig úgy kapunk, hogy rögzítjük $\overline{G}$-nek egy $\nu(\overline{G})$ élből álló, M maximális párosítását, és minden csúcsot különböző színnel színezünk, kivéve, hogy M minden élének végpontjai azonos színt kapnak. Ezáltal a felhasznált színekben az n-hez képest $\nu(\overline{G})$ megtakarítást érünk el. □

Tétel: Páros gráf élgráfja perfekt.

Biz: Ha G páros gráf, akkor $L(G)$ élgráfjának tetszőleges feszített részgráfja azonos G egy alkalmas részgráfjának élgráfjával, azaz szintén egy páros gráf élgráfja. Elegendő tehát azt bizonyítani, hogy $\chi(L(G)) = \omega(L(G))$ tetszőleges G páros gráfra.

Mivel G háromszög-mentes, ezért $L(G)$ minden klikkje G egy csúcsból induló éleinek felel meg, így $\omega(L(G)) = \Delta(G)$. Kőnig páros gráfok élszínezéséről szóló tételének felhasználásával $\omega(L(G)) = \Delta(G) = \chi'(G) = \chi(L(G))$ következik. □

Tétel: Páros gráf élgráfjának komplementere perfekt.

Biz: Ha G páros gráf, akkor $\overline{L(G)}$ feszített részgráfja nem más, mint $\overline{L(G')}$, ahol G' a G alkalmas részgráfja. Mivel G' páros, ezért elegendő azt igazolni, hogy $\chi(\overline{(L(G))}) \leq \omega(\overline{L(G)})$ tetszőleges G páros gráfra (a másik irányú egyenlőtlenség triviális).

A Kőnig tétel alapján $\omega(\overline{L(G)}) = \alpha(L(G)) = \nu(G) = \tau(G)$, ezért elegendő $\tau(G)$ színnel kiszínezni $\overline{L(G)}$-t. Legyen $U \subset V(G)$ egy $\tau(G)$ pontból álló lefogó ponthalmaz, és válasszunk G minden egyes e éléhez e-nek egy U-beli végpontját. Ha minden élt a kiválasztott végpontnak megfelelően színezünk, akkor $\tau(G)$ színt használunk, és az azonos színű élek páronként szomszédosak, azaz a nekik megfelelő pontok $\overline{L(G)}$-ben függetlenek. Tehát ez csakugyan egy $\tau(G)$ színnel történő színezése $\overline{L(G)}$-nek. □

További példát is adunk perfekt gráfra, de ehhez értelmezzük a rendezést.

Def: Ha D irányított gráf, akkor $u \xrightarrow{D} v$ jelöli azt, hogy u-ból vezet v-be D-ben irányított út.

A D irányított gráf *aciklikus*, ha nem tartalmaz irányított kört.

A D irányított gráf v csúcsa *forrás (nyelő)*, ha v-be nem fut be (v-ből nem indul ki) G-nek éle.

Állítás: Ha a D véges, irányított gráf aciklikus, akkor létezik forrása és nyelője is.

Biz: Tetszőleges pontból kiinduló sétát az aciklikus tulajdonság miatt sosem érinthet korábban érintett pontot, ezért a séta előbb-utóbb elakad egy nyelőben. A megfordított éleken haladó séta hasonló okok miatt forrásba jut. □

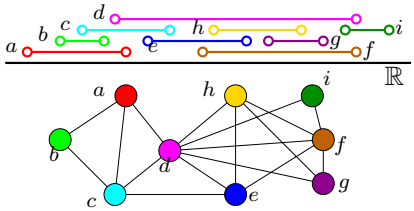
A $\preceq$ relációt az X halmazon *részbenrendezésnek* nevezzük, ha létezik az X ponthalmazon egy aciklikus D irányított gráf, melyre $(x \preceq y) \iff (x \xrightarrow{D} y)$. (Az x-t akkor tekintjük kisebbnek y-nál, ha x-ből irányított úton y-ba juthatunk.)late A $\preceq$ részbenrendezés szerint x és y *összehasonlítható*, ha $x \preceq y$ vagy $y \preceq x$.

Megjegyzés: A részbenrendezés szokásos definíciója három tulajdonságot kíván meg:
(1) *reflexivitás*: $x \preceq x \qquad \forall x \in X$, (2) *antiszimmetria*: ha $x \preceq y$ és $y \preceq x$, akkor $x = y$, valamint
(3) *tranzitivitás*: ha $x \preceq y$ és $y \preceq z$, akkor $x \preceq z$.
Könnyű ellenőrizni, hogy aciklikus D irányított gráf esetén a $\preceq := \xrightarrow{D}$ reláció kielégíti a fenti 3 feltételt. Másrészt az is közvetlenül adódik, hogy ha $\preceq$ a fenti 3 tulajdonságot teljesítő reláció, akkor az X halmazon bevezetve minden xy élt, melyre $y \neq x \preceq y$, egy olyan aciklikus D irányított gráfot kapunk, melyre $\preceq = \xrightarrow{D}$. Tehát a részbenrendezés hagyományos definíciója egyenértékű a fenti, irányított gráfossal.

Példa:
1. A valós számok a $\leq$ rendezéssel. (Bármely 2 szám összehasonlítható, tehát ez egy *teljes renezés.*)
2. Az X halmaz részhalmazain értelmezett $\subseteq$ reláció. (Vannak nem összehasonlítható elemek.)
3. Az $\mathbb{N}$ halmazon az oszthatóság. (Vannak nem összehasonlítható elemek.)

4. Intervallumrendezés: $I_1, I_2, \ldots$ valós intervallumok. $I_i \preceq I_j$, ha $I_i = I_j$, vagy $x_i < x_j$ minden $x_i \in I_i$, $x_j \in I_j$ esetén. (Az I_j intervallum teljes egészében jobbra van I_i-től.)

Def: Legyen $\preceq$ az X halmaz részbenrendezése. A $G_\preceq$ *összehasonlítási gráf* csúcshalmaza X, élei pedig azon uv-k, melyekre $u \neq v$, továbbá u és v összehasonlítható: $x \preceq y$ vagy $y \preceq x$.



Példa: Legyenek az $I_1, I_2, \ldots$ valós intervallumok a G gráf csúcsai, és fusson az I_i és I_j csúcsok között él, ha $I_i \cap I_j \neq \emptyset$. (Az ilyen típusú gráfok neve *intervallumgráf.*)

Megjegyzés: A G intervallumgráf komplementere az intervallumrendezésnek megfelelő összehasonlítási gráf.

Tétel: Ha $\preceq$ a véges X halmaz részbenrendezése, akkor a $G_\preceq$ összehasonlítási gráf perfekt.

Biz: Először megfigyeljük, hogy $G_\preceq$ minden feszített részgráfja is összehasonlítási gráf. Valóban: a $G_\preceq$ ponthalmazának egy U részhalmaza által feszített gráf nem más, mint az U-ra megszorított $\preceq|_U$ részbenrendezés $G_{\preceq|_U}$ összehasonlítási gráfja. (Az világos, hogy a $\preceq|_U$ megszorítás is részbenrendezés.)

A tétel igazolásához tehát annyit kell megmutatni, hogy ha $G_\preceq$ összehasonlítási gráf, akkor $\omega(G_\preceq) \geq \chi(G_\preceq)$. (Itt felhasználtuk a korábban általában bizonyított $\omega(G_\preceq) \leq \chi(G_\preceq)$ egyenlőtlenséget.) Legyen D olyan aciklikus irányított gráf, melyre $\preceq = \overset{D}{\longrightarrow}$. Legyen V_1 a D gráf forrásainak halmaza és $D_1 := D - V_1$, legyen V_2 a D_1 forrásainak halmaza, és $D_2 := D_1 - V_2$, stb. Tegyük fel, hogy $V(G) = V_1 \cup V_2 \cup \ldots \cup V_k$. Nyilván a $V_1, V_2, \ldots V_k$ ponthalmazok egyikén belül sem fut $G_\preceq$-nek éle, tehát $G_\preceq$ k-színezhető, azaz $\chi(G_\preceq) \leq k$. A konstrukció miatt minden $u_i \in V_i$-hez van $u_{i-1} \in V_{i-1}$, melyre $u_{i-1}u_i \in E(D)$. Létezik tehát D-ben egy $v_1v_2 \ldots v_k$ irányított út V_1-ből V_k-ba. A $v_1, v_2, \ldots v_k$ pontok $G_\preceq$-ben klikket alkotnak, tehát $\omega(G_\preceq) \geq k \geq \chi(G_\preceq)$. □

Gyenge perfekt gráf tétel: Ha G perfekt, akkor (és csak akkor) $\overline{G}$ is perfekt.

Köv.: Minden intervallumgráf perfekt.

Biz: Az intervallumgráf komplementere az intervallumrendezés összehasonlítási gráfja, tehát perfekt. A gyenge perfekt gráf tétel miatt az intervallumgráf is perfekt. □

A gyenge perfekt gráf tételt először Lovász bizonyította be, az alábbi állítás igazolásával.

Lovász tétele: A G gráf perfekt $\iff$ G minden G' feszített részgráfjára $\alpha(G') \cdot \omega(G') \geq |V(G')|$.

A szükségesség bizonyítása: Mivel G egy $\chi(G)$-színezésének $V_1, V_2, \ldots$ színosztályai diszjunkt független halmazok, ezért $|V(G)| = |V_1| + |V_2| + \ldots \leq \alpha(G) \cdot \chi(G)$. Ha G' a G perfekt gráf feszített részgráfja, akkor $\chi(G') = \omega(G')$ miatt $|V(G')| \leq \alpha(G') \cdot \chi(G') = \alpha(G') \cdot \omega(G')$. □

Gasparian bizonyítása Lovász tételére: Az elégségességet igazoljuk. A szükségességet láttuk, így elegendő azt megmutatni, hogy ha G minimális imperfekt (azaz G nem perfekt, de minden valódi feszített részgráfja az), akkor $\alpha(G) \cdot \omega(G) < |V(G)|$. Legyen $\alpha := \alpha(G)$, $\omega := \omega(G)$. Figyeljük meg, hogy ha $A \subseteq V(G)$ független, akkor $\omega + 1 \leq \chi(G) \leq \chi(G - A) + 1 = \omega(G - A) + 1 \leq \omega + 1$, tehát $\omega = \omega(G - A) = \chi(G - A)$. Létezik tehát G minden α méretű A független halmazához egy ω méretű, A-tól diszjunkt $K(A)$ klikk G-ben.

Legyen $A_0 = \{a_1, a_2, \ldots, a_\alpha\}$ a G egy α méretű független halmaza. $G - a_i$ perfekt, és $\chi(G - a_i) = \omega(G - a_i) = \omega$, tehát legyenek az $A_i^1, A_i^2, \ldots A_i^\omega$ független halmazok a $G - a_i$ gráf egy ω-színezésének színosztályai. Vegyük észre, hogy az ω méretű $K(A_i^j)$ klikk a $\omega - 1$ db A_i^k $(k \neq j)$ színosztály mindegyikét legfeljebb 1 pontban metszi, ezért $|K(A_i^j) \cap A_i^k| = 1$ és $a_i \in K(A_i^j)$. Mivel a $K(A_i^j)$ klikk az A_0 függetlent sem metszheti 2 pontban, ezért $l \neq i$-re $a_l \notin K(A_i^j)$, vagyis $K(A_i^j) \subseteq G - a_l$. Az ω méretű $K(A_i^j)$ klikk a $G - a_l$ gráf ω-színezésének $A_l^1, A_l^2, \ldots A_l^\omega$ színosztályait tehát $1-1$ pontban metszi. Az is világos, hogy az ω méretű $K(A_0)$ klikk diszjunkt a_i-től, azaz a $G - a_i$ gráf ω-színezésének $A_i^1, A_i^2, \ldots A_i^\omega$ színosztályait $1-1$ pontban metszi.

Legyen $\mathcal{A}$ az a mátrix, melynek $\alpha \cdot \omega + 1$ sora az

$$A_0, A_1^1, A_1^2, \ldots A_1^\omega\, A_2^1, A_2^2 \ldots, A_\alpha^\omega$$

független halmaznak megfelelő incidenciavektorok, a $\mathcal{K}$ mátrix $\alpha \cdot \omega + 1$ sora pedig legyen rendre a

$$K(A_0), K(A_1^1), K(A_1^2), \ldots K(A_1^\omega), K(A_2^1), K(A_2^2) \ldots, K(A_\alpha^\omega)$$

klikkek incidenciavektora. Mindkét mátrix tehát $(\alpha \cdot \omega + 1) \times |V(G)|$ méretű, így az $(\alpha \cdot \omega + 1) \times (\alpha \cdot \omega + 1)$ méretű $M = \mathcal{A} \cdot \mathcal{K}^T$ szorzatmátrix rangja is legfeljebb $|V(G)|$. Márpedig M minden eleme a megfelelő független halmaz és klikk közös elemeinek számát tartalmazza, azaz M főátlójában 0-k, minden főátlótól különböző helyén pedig 1-esek állnak. Könnyen látható, hogy M rangja $\alpha \cdot \omega + 1$, azaz $\alpha \cdot \omega < |V(G)|$. □

Az intervallumgráfok perfektségét közvetlenül (a gyenge perfekt gráf tétel nélkül) is bebizonyítjuk. Ehhez a következő segédtételre lesz szükség.

Lemma: Tegyük fel, hogy a G gráf olyan, hogy minden feszített részgráfjának van *szimpliciális csúcsa*, azaz olyan v pontja, melynek szomszédai klikket alkotnak G-ben. Ekkor G perfekt.

Biz: A G gráf n pontszáma szerinti indukcióval bizonyítunk. Ha $n = 1$, akkor G perfekt, az állítás igaz. Tegyük fel, hogy a legfeljebb n pontú gráfokra igaz a lemma, és legyen az állításban leírt tulajdonságú G gráfnak $n+1$ csúcsa. A G gráf minden valódi feszített részgráfja legfeljebb n csúccsal rendelkezik, ezért igaz rájuk az indukciós állítása. Vagyis csupán annyit kell bizonyítanunk, hogy $\chi(G) = \omega(G)$ áll.

Legyen v a G szimpliciális csúcsa és legyen $G' = G - v$ az e pont törlésével keletkező, n csúcsú gráf! Mivel v törlése legfeljebb eggyel csökkenti a klikkszámot, ezért $\omega(G) \geq \omega(G') \geq \omega(G) - 1$. Ha tehát $\omega(G) > \omega(G')$, akkor $\omega(G) = \omega(G') + 1 = \chi(G') + 1 \geq \chi(G)$, ahol a második egyenlőség azért igaz, mert a G' gráfra teljesül az indukciós állítás, az egyenlőtlenség pedig abból következik, hogy ha G'-t kiszínezzük $\chi(G')$ színnel, és v-nek egy újabb színt adunk, akkor G egy jó színezését kapjuk. Ezt összevetve a minden gráfra teljesülő, korábban bizonyított $\chi(G) \geq \omega(G)$ egyenlőtlenséggel, $\chi(G) = \omega(G)$ adódik.

Az $\omega(G) = \omega(G')$ esetet kell még ellenőriznünk. Mivel v a szomszédaival együtt is klikket alkot, ezért v-nek legfeljebb $\omega(G) - 1$ szomszédja lehet. Innen $\omega(G) = \omega(G') \geq \chi(G) \geq \omega(G)$ adódik, ahol az utolsó egyenlőtlenség a szokásos triviális becslés. Az utolsó előtti egyenlőtlenség magyarázata, hogy G' az indukciós állítás szerint kiszínezhető $\omega(G')$ színnel, de v-nek $\omega(G')$-nél kevesebb szomszédja van, tehát v számára is marad felhasználható szín. Ez G-nek egy $\omega(G')$ színnel történő színezését adja, ennél G kromatikus száma nem lehet nagyobb. □

Be lehet bizonyítani, hogy az ú.n. *merevkörű* gráfok (melyekben 3-nál hosszabb körök nem fordulhatnak elő feszített részgráfként) rendelkeznek szimpliciális csúccsal. Innen azonnal adódik, hogy a merevkörű gráfok perfektek.

Az intervallumgráfok perfektségének bizonyítása: A fenti lemma miatt csupán azt kell igazolni, hogy az intervallumgráf tetszőleges feszített részgráfjának van szimpliciális csúcsa. Mivel az intervallumgráf minden feszített részgráfja intervallumgráf, ezért elegendő csupán annyit megmutatni, hogy tetszőleges intervallumgráfnak létezik szimpliciális csúcsa. Legyen G tehát egy intervallumgráf, és legyenek $I_1, I_2, \ldots$ a G-t meghatározó intervallumok. Feltehetjük, hogy az I_1 intervallum jobbvégpontja a legkisebb az adott intervallumok jobbvégpontjai között. Állítjuk, hogy a G gráf I_1-nek megfelelő csúcsa szimpliciális. Ehhez mindössze azt kell igazolni, hogy az I_1-t metsző intervallumok egymást is páronként metszik. Mivel minden I_j intervallum jobbvégpontja jobbra van I_1 jobbvégpontjától, ezért minden I_1-t metsző intervallum tartalmazza I_1 jobbvégpontját, és éppen ezt akartuk bizonyítani. □

Megjegyzés: A fenti bizonyítás módszere alkalmas a tétel általánosítására, és intervallumgráfok helyett részfagráfokról megmutatni, hogy perfektek. Egy G gráf *részfagráf*, ha csúcsai egy F fa részfáinak felelnek meg úgy, hogy két csúcs között pontosan akkor fut él, ha a megfelelő két részfának létezik közös csúcsa. Ha F egy út, akkor az F-hez tartozó részfagráf intervallumgráf, és minden intervallumgráf részfagráfja egy alkalmas útnak. Ha tekintjük F egy v csúcsát, akkor vagy minden részfa tartalmazza v-t, és akkor G egy klikk, ami perfekt, vagy létezik egy olyan T részfa, aminek a v-hez legközelebbi u csúcsa v-től a lehető legtávolabb van. Könnyen látható, hogy minden T-t metsző részfa tartalmazza u-t, vagyis a G gráf T-nek megfelelő csúcsa szimpliciális.

Perfekt gráf tétel: (Chudnovsky, Robertson, Seymour és Thomas) Egy G véges gráf pontosan akkor perfekt, ha sem G, sem $\overline{G}$ nem feszít legalább 5 hosszú, páratlan kört. □

Történelem A perfekt gráf tételt Claude Berge már 1960-ban sejtette. Széles körben ismertté válását követően népes matematikushadsereg próbálta bebizonyítani, de csak részeredményeket sikerült igazolni. A sejtés fokozatosan a gráfelmélet egyik centrális jelentőségű megoldatlan problémájává vált: számos fontos kérésről derült ki, hogy szorosan kapcsolódik a problémához. A 2002-ben megtalált bizonyítás, mely jelentős részben az akkor 25 éves Maria Chudnovsky nevéhez fűződik, komoly áttörés a gráfelméletben. Maria időközben több nehéz problémát oldott, ezzel is bebizonyítva, hogy részéről nem véletlen szerencse volt a sejtés igazolása.

7. A Turán-tételkör

Az extremális gráfelmélet olyasfajta kérdéseket vizsgál, hogy mekkora lehet egy adott gráfparaméter, ha a gráfra különböző megkötéseket teszünk. A számos ilyen kérdés közül egy lehetséges annak vizsgálata, hogy hogyan alakul egy gráf élszáma, ha bizonyos részgráfokat kizárunk. Az egyik legegyszerűbb eset, ha a nagy klikkek a kizárt részgráfok.

Mantel tétele: Ha az n-pontú, egyszerű G gráf háromszögmentes (azaz $\omega(G) \leq 2$), akkor $|E(G)| \leq \left\lfloor \frac{n}{2} \right\rfloor \cdot \left\lceil \frac{n}{2} \right\rceil$.

Biz: Legyen v a G-nek egy $\Delta(G)$-fokú pontja. Mivel G nem tartalaz K_3-t, az $N(v)$ egy $\Delta(G)$ méretű független ponthalmaz, ahonnan $\alpha(G) \geq \Delta(G)$. Gallai tételét alkalmazva

$$|E(G)| \leq \tau(G)\Delta(G) \leq \tau(G)\alpha(G) = \tau(G)(n - \tau(G)) \leq \left\lfloor \frac{n}{2} \right\rfloor \cdot \left\lceil \frac{n}{2} \right\rceil$$

adódik. □

A tételbeli korlát elérhető, ha pl. a gráf egy olyan teljes páros gráf, melynek osztályaiba a lehető legegyenletesebben osztottuk el a pontokat, azaz úgy, hogy a két színosztály mérete legfeljebb eggyel különbözzön. Igaz az is, hogy ez az egyetlen extrém gráf, de ezt általánosabban is be tudjuk bizonyítani.

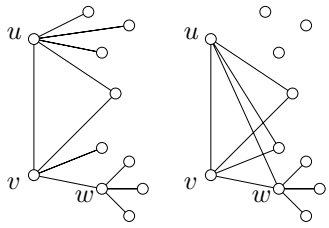
Def: A G gráfot *teljes m-osztályú gráf*nak nevezzük, ha G egyszerű, és G komplementere m db diszjunkt klikkből áll. Úgy is mondhatjuk, hogy G pontjai m osztályba sorolhatóak úgy, hogy uv pontosan akkor éle G-nek, ha u és v különböző osztályba esnek.

Def: Az *n-pontú, m-osztályú Turán-gráf* olyan n-pontú, m-osztályú teljes gráf, mely komplementerében a klikkek mérete legfeljebb eggyel tér el egymástól. (Azaz, ha $n = qm + r$, ahol $0 \leq r < m$, akkor a gráfnak r db $q+1$ méretű és $m - r$ db q méretű osztálya van.) A fenti Turán-gráfot $T_{n,m}$ jelöli.

Turán tétele: Ha az egyszerű G gráf nem tartalmaz K_{m+1}-gyel izomorf részgráfot (azaz $\omega(G) \leq m$), akkor $|E(G)| \leq |E(T_{n,m})|$, és egyenlőség pontosan akkor áll, ha $G \cong T_{n,m}$.

Biz: Kényelmes áttérni a komplementerre, azaz azt igazolni, hogy ha a $H := \overline{G}$ egyszerű gráfban nincs $m+1$ ftn pont (vagyis $\alpha(H) \leq m$), akkor $|E(H)| \geq |E(\overline{T_{n,m}})|$, és egyenlőség pontosan akkor áll, ha a H gráf m diszjunkt klikkből áll, melyek mérete legfeljebb eggyel tér el egymástól.

Legyen H tehát olyan n-pontú gráf, melyre $\alpha(H) \leq m$, és $|E(H)|$ ezen belül minimális. Vegyük észre, hogy a következő operáció nem növeli $\alpha(H)$-t. Ha u és v szomszédos pontok, akkor töröljük az u-ból induló éleket, és u-t összekötjük v szomszédaival és v-vel. Ha ugyanis az operáció után létrejön egy F ftn ponthalmaz, akkor F u és v közül legfeljebb egyet tartalmaz. Ha tehát F nem volt ftn korábban, akkor $u \in F$, de ekkor $F \setminus \{u\} \cup \{v\}$ korábban szintén ftn volt. Ha u fokszáma nagyobb volt v fokszámánál, akkor a fenti operáció H élszámát csökkentette.



Mivel H-nak minimális számú éle volt, ezért ha u és v szomszédos H-ban, akkor egyikük fokszáma sem csökkenhet az operáció során, tehát u és v fokszáma megegyezik. Eszerint H minden komponense reguláris gráf. Tegyük fel, hogy valamelyik komponens nem klikk. Ekkor találunk olyan u, v, w pontokat, melyekre $uv, vw \in E(G) \not\ni uw$. Ha elvégezzük a fenti operációt u és v pontokra, akkor u fokszáma nem változik, de w fokszáma növekszik az uw él behúzása miatt. Ezáltal a komponens nem marad reguláris egy minimális élszámú ellenpéldában, ami ellentmondás.

Azt kaptuk, hogy H minden komponense klikk. $\alpha(H) \leq m$ miatt világos, hogy H-nak legfeljebb m komponense van. Ha H komponenseinek száma m-nél kisebb, akkor egy komponenst két komponensre vágva az élszám tovább csökkenthető úgy, hogy $\alpha(H) \leq m$ igaz marad, tehát H pontosan m klikk-komponensből áll. Ha van két olyan klikk-komponens, melyek mérete legalább 2-vel különbözik, akkor a nagyobb komponensből egy pontot a kisebbe átrakva H élszáma csökken, $\alpha(H)$ nem változik. Ez is ellentmondás, vagyis H csakugyan $T_{n,m}$ komplementere, és éppen ezt akartuk bizonyítani. □

A Turán tétel alapján, ha egy gráfban nincs nagy klikk, és a gráfnak a lehető legtöbb éle van, akkor a gráfban nagy független halmazok találhatóak. Felmerül a kérdés, vajon ez mindig igy van-e, azaz lehetséges-e, hogy egy gráfban a klikkek és a ftn halmazok is kicsik. Pontosítjuk a kérdést: Igaz-e, hogy tetszőleges k és l pozitív egészekhez létezik egy $f(k,l)$ egész azzal a tulajdonsággal, hogy ha egy G gráfnak legalább $f(k,l)$ pontja van, akkor vagy $\alpha(G) > k$ vagy $\omega(G) > l$ (vagy mindkét egyenlőtlenség) teljesül. Ramsey megmutatta, hogy létezik ilyen $f(k,l)$ mennyiség. A tételt és bizonyítását az extremális gráfelméletet egy másik vonulatának felvillantása okán közöljük.

Ramsey tétele: Ha $|V(G)| \geq 2^{k+l}$, akkor $\alpha(G) \geq k$, vagy $\omega(G) \geq l$.

Biz: $k+l$ szerinti indukcióval bizonyítunk, $k+l=1$ esetén az állítás triviális: egy legalább kétpontú gráfban vagy van két összekötött, vagy van két összekötetlen pont. Tegyük fel, hogy $(k+l-1)$-re már igazoltuk a tételt.

Legyen $|V(G)| = 2^{k+l}$, és legyen v a G egy pontja. Az indukciós feltevés szerint, ha $d(v) \geq 2^{k+l-1}$, akkor a v szomszédai feszítette részgráf vagy tartalmaz k méretű függetlent, vagy $l-1$ méretű klikket, mely utóbbi v-vel együtt G egy l méretű klikkjét alkotja.

Egyébként $d(v) \leq 2^{k+l-1} - 1$, vagyis v legalább 2^{k+l-1} ponttal nincs összekötve G-ben. Az indukciós feltevés miatt ezek a pontok vagy feszítenek egy $k-1$ méretű ftn halmazt (mely v-vel együtt G egy k méretű független halmazát alkotja), vagy található a nemszomszédok között l pont, mely klikket feszít. A tétel állítása ebben az esetben is teljesül. □

A Ramsey tétel egy következménye, hogy $\min(\alpha(G), \omega(G)) \geq \frac{\log_2(|V(G)|)}{2}$ teljesül tetszőleges, véges G gráfra.

8. Oszthatóság, prímek

Def: Az a, b egész számokról azt mondjuk, hogy a *osztja* b-t, vagy másképpen, hogy b az a *többszöröse*, (jelölése $a \mid b$), ha $b = aq$ valamely q egész számra. Az n szám osztóinak halmazát $D(n)$ jelöli. Világos, hogy $n \neq 0$ esetén $\pm 1, \pm n \in D(n)$. A $D(n) \setminus \{\pm 1, \pm n\}$ halmaz elemeit n *valódi osztóinak* nevezzük.

Megfigyelés: (1) Ha $a \mid b$ akkor tetszőleges $c \in \mathbb{Z}$-re $a \mid bc$ ill. $ac \mid bc$.
(2) Bármely $a \mid b$ esetén $(a \mid c) \Longleftrightarrow (a \mid b + c)$.
(3) Tetszőleges a egészre $D(a) = D(|a|)$. □

Def: A $p > 1$ egész szám *felbonthatatlan*, ha $p = a \cdot b$ $(a, b \in \mathbb{N}) \Rightarrow a = p$ vagy $b = p$.
Az $n > 1$ egész szám *összetett*, ha nem felbonthatatlan, azaz van valódi osztója. (Más szóval, előáll két, nem feltétlenül különböző valódi osztójának szorzataként.)
A $p > 1$ egész szám *prím*, ha $p \mid ab$ $(a, b \in \mathbb{N}) \Rightarrow p \mid a$ vagy $p \mid b$. (Más szóval, azok a számok prímek, melyek egészek egy szorzatát pontosan akkor osztják, ha valamelyik tényezőt osztják.)

Állítás: Ha p prím, akkor p felbonthatatlan.

Biz: Ha $p = ab$, akkor $p \mid ab$, ezért p prímvolta miatt $p \mid a$ vagy $p \mid b$. Tudjuk még, hogy $p \geq a$ és $p \geq b$. Ha $a \leq p \mid a$, akkor $a = p$, egyébként $b \leq p \mid b$, így $b = p$. Tehát p valóban felbonthatatlan. □

A következő cél annak igazolása, hogy minden felbonthatatlan szám prím. Ennek érdekében van szükség a legnagyobb közös osztó fogalmára.

Def: Az $a_1, a_2, \ldots, a_k \in \mathbb{N}$ számok *közös osztói*nak halmaza, $D(a_1, a_2, \ldots, a_k) := D(a_1) \cap D(a_2) \cap \ldots \cap D(a_k)$. Ha $a_i \neq 0$ valamelyik i-re, akkor a $D(a_i)$ halmaz felülről korlátos, így az $(a_1, a_2, \ldots, a_k) := \max D(a_1, a_2, \ldots, a_k)$ definíció értelmes, és az $a_1, a_2, \ldots, a_k$ számok *legnagyobb közös osztóját* definiálja. Az a, b számokat *relatív prímeknek* mondjuk, ha $(a, b) = 1$.

Megfigyelés: (1) Tetszőleges $a \neq 0$ egészre $D(a, 0) = D(a)$ és $(a, 0) = |a|$, hisz $D(0) = \mathbb{Z}$.
(2) Tetszőleges q egész szám esetén $D(a, b) = D(a, b + aq)$. Speciálisan $(a, b) = (a, b + aq)$ □

A fenti megfigyelés (2) része egyben eljárást is ad arra nézve, hogyan lehet a és b (nemnegatív) egész számok legnagyobb közös osztóját meghatározni. Ha $a \leq b$, akkor (a, b) meghatározása helyett elegendő $(a, b) = (a, b-a)$ meghatározása, és iterálhatjuk ezt a lépést, azaz azt, hogy a két szám közül a nagyobból kivonjuk a kisebbet. Ha a kivonás után a és b nagyságrendje nem változik, akkor ismét a-t vonjuk ki $b - a = b'$-ből, ha a nagyságrend megfordul, akkor b'-t vonjuk ki a-ból, s.í.t. Persze okosabb, ha a-t mindjárt annyiszor vonjuk ki, ahányszor csak lehet, azaz $\left\lfloor \frac{b}{a} \right\rfloor$-szer. Más szóval, felírjuk b-t $b = q \cdot a + r$ alakban, ahol q egész, és $0 \leq r < a$, majd $(a, b) = (a, r)$ lépést végzünk. Ez a lépés az alapja az alábbi módszernek.

Euklideszi algoritmus: Legyen $a, b \in \mathbb{N}$, $b > a$. Definiáljuk az $a_0 := a, a_1, a_2, \ldots$ ill. $b_0 := b, b_1, b_2, \ldots$ számokat úgy, hogy $b_i = q_i \cdot a_i + a_{i+1}$, ill. $b_{i+1} := a_i$ legyen, ahol q_i-t úgy választjuk, hogy $0 \leq a_{i+1} < a_i$ teljesüljön. Az eljárás akkor ér véget, ha $a_{k+1} = 0$.

A fentiek szerint $(a, b) = (a_0, b_0) = (a_1, b_1) = \ldots = (a_{k+1}, b_{k+1}) = (0, b_{k+1}) = b_{k+1} = a_k$ adódik a legnagyobb közös osztóra. Az eljárás azért ér véget, mert az (a_i) sorozat nemnegatív egészekből áll és csökken, tehát az Euklideszi algoritmus lépésszámára $|a_0|$ felső becslés.

Megjegyzés: Az Euklideszi algoritmus valójában ennél sokkal hatékonyabb: belátható, hogy $a_{i+2} \leq \frac{a_i}{2}$, ezért a lépésszám lényegében $\log_2(a_0)$, vagyis a_0 bináris jegyeinek számával arányos. Sőt: ha az Euklideszi algoritmusban a_i-t úgy választjuk, hogy $-\left\lfloor \frac{a_i}{2} \right\rfloor \leq a_{i+1} < \left\lceil \frac{a_i}{2} \right\rceil$ teljesüljön (amit szintén megtehetünk), akkor $|a_{i+1}| \leq |\frac{a_i}{2}|$ is teljesülni fog, amitől az algoritmus elméleti hatékonysága tovább növekszik.

Köv.: Legyenek a, b tetszőleges pozitív egészek.

(1) Léteznek m és n egészek úgy, hogy $(a, b) = na + mb$ teljesüljön, azaz a a és b legnagyobb közös osztója felírható a és b ú.n. *egész kombinációjaként.*

(2) Ha $d \in D(a, b)$, akkor $d \mid (a, b)$. Azaz $D(a, b) = D((a, b))$, más szóval, a közös osztók halmaza azonos a legnagyob közös osztó oszóinak halmazával.

Biz: (1) Számítsuk ki az (a, b) legnagyobb közös osztót az Euklideszi algoritmussal! Világos, hogy $a_0 = 1 \cdot a + 0 \cdot b$ és $b_0 = 0 \cdot a + 1 \cdot b$ felírható egész kombinációként. Könnyen látható, hogy ha a_i felírható az a és b egész kombinációjaként (azaz $a_i = b_{i+1} = n_i a_0 + m_i b_0$ alakban, ahol $n_i, m_i \in \mathbb{Z}$), akkor a_{i+1} is felírható bizonyos n_{i+1} és m_{i+1} egész együtthatók meghatározta egész kombinációként. Teljes indukcióval tehát $a_k = (a, b)$ is előáll a és b egész kombinációjaként.

(2) A tétel imént igazolt (1) része miatt $(a, b) = na + mb$ alkalmas n, m egészekre. Ha tehát $d \mid a$ és $d \mid b$, akkor $d \mid na + mb = (a, b)$ is teljesül. □

Tétel: Minden felbonthatatlan szám prím.

Biz: Legyen p felbonthatatlan, és tegyük fel, hogy $p \mid ab$. Azt szeretnénk igazolni, hogy $p \mid a$ vagy $p \mid b$. Tekintsük a $d := (p, a)$ legnagyobb közös osztót. Mivel $d \mid p$, és p-nek nincs valódi osztója, ezért $d = 1$ vagy $d = p$ lehet. Utóbbi esetben $p \mid a$, kész vagyunk. Egyébként $d = 1$. Ha most indirekt feltesszük, hogy $p \nmid b$, akkor $(p, b) = 1$ teljesül. Ezért az Euklideszi algoritmus utáni következmény miatt az 1 előáll kétféle egész kombinációként: $ka + lp = 1 = mb + np$. Innen $1 = 1 \cdot 1 = (ka + lp) \cdot (mb + np) = X \cdot ab + Y \cdot p$, ahol X, Y egészek. Márpedig $p \mid ab$ miatt $p \mid X \cdot ab + Y \cdot p = 1$, ellentmondás. □

Végre ki tudunk mondani valami fontosat.

A számelmélet alaptétele: Minden $1 < n \in \mathbb{N}$ szám (a tényezők sorrendjétől eltekintve) egyértelműen bontható fel prímszámok szorzatára.

Biz: n szerinti indukcióval bizonyítunk. A tétel $n = 2$-re világos. Tegyük fel, hogy minden, k-nál kisebb számra már bizonyítottunk, és legyen $n = k$. Ha n prím, akkor kész vagyunk, hisz egytényezős szorzatunk van, ami egyértelmű felbontás, hisz egyetlen prím sem áll elő két egynél nagyobb szám szorzataként.

Különben n-nek van egy p prímosztója, hisz (összetett szám lévén) van valódi osztója, és a legkisebb valódi osztója szükségképpen prím. Az $n = pn'$ felbontásbeli n' szám az indukciós feltevés miatt egyértelműen bomlik prímek szorzatára: $n' = \prod_{i=1}^{k} p_i^{\alpha_i}$. Innen megkaptunk egy $n = p \prod_{i=1}^{k} p_i^{\alpha_i}$ prímek szorzataként történő előállítást. Tegyük fel, hogy $n = \prod_{j=1}^{l} q_j$ is egy prímek szorzatára bontás. Mivel $p \mid n$, p prímtulajdonsága miatt $p = q_m$ valamely $m = 1, 2, \ldots, l$-re. Ám ekkor $n' = \prod_{i=1}^{k} p_i^{\alpha_i} = \prod_{j \neq m} q_j$, így az n'-re már igazolt egyértelműség miatt n is egyértelműen bomlik prímtényezők szorzatára. □.

Def: Az n szám *kanonikus alakján* az n prímtényezők szorzataként való előállítását értjük. Az n pozitív osztóinak számát $d(n)$, pozitív osztóinak összegét $\sigma(n)$ jelöli.

Egy n szám kanonikus alakja sok hasznos információt ad n-ről, pl. az osztóiról.

Tétel: Legyen $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ az n szám kanonikus alakja. Ekkor n pozitív osztóinak száma $d(n) = \prod_{i=1}^{k} (\alpha_i + 1)$, az n pozitív osztóinak összege pedig $\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$.

Biz: Bármely $d \mid n$ osztó kanonikus alakja olyan, hogy azt további prímekkel megszorozva n kanonikus alakját kapjuk, azaz $d = \prod_{i=1}^{k} p_i^{\beta_i}$, ahol $0 \leq \beta_i \leq \alpha_i$ teljesül minden i-re. Világos, hogy minden osztóhoz tartozik egy $(\beta_1, \ldots, \beta_k)$ kitevősorozat, és különböző kitevősorozatok (a prímfelbontás egyértelműsége miatt) különböző osztókhoz tartoznak. (A $d = 1$ osztóhoz pl. a csupa-0 sorozat tartozik.) Vagyis a pozitív osztók száma azonos a lehetséges $(\beta_1, \ldots, \beta_k)$ sorozatok számával, ahonnan $d(n) = \prod_{i=1}^{k} (\alpha_i + 1)$ adódik, hisz minden β_i a többi kitevőtől függetlenül $\alpha_i + 1$ érték valamelyikét veszi fel.

Világos, hogy az osztók összege $\sigma(n) = (1 + p_1 + p_1^2 + \ldots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \ldots + p_2^{\alpha_2}) \ldots (1 + p_k + p_k^2 + \ldots + p_k^{\alpha_k}) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1}-1}{p_i-1}$, hisz minden osztó egyértelműen áll elő, mint az első szorzat egy kifejtési tagja, míg a második egyenlőség a mértani sorozatok összegzésével adódik. □

Def: Ha a és b egész számok, akkor $[a, b]$ jelöli a és b legkisebb közös többszörösét, azaz azt a legkisebb pozitív egész n számot, amire $a \mid n$ és $b \mid n$ teljesül.

Megfigyelés: Legyenek a és b pozitív egészek. Ekkor (a, b) kanonikus alakját úgy kapjuk, hogy az a és b kanonikus alakjában szereplő közös prímeket a szereplő kisebb kitevőre emelve összeszorozzuk. Az $[a, b]$ legkisebb többszörös kanonikus alakja úgy áll elő, hogy az a vagy b kanonikus alajában szereplő összes prímet a felbontásbeli nagyobb kitevőre emelve összeszorzunk. Végül $ab = (a, b) \cdot [a, b]$.

Biz: Az első két állítás következik az osztó kanonikus alakjára vonatkozó korábbi megfigyelésünkből, a harmadik állítás pedig közvetlenül adódik az első kettőből. □

Tétel: A prímszámok száma végtelen.

Biz: Elegendő azt megmutatni, hogy minden $2 \leq n \in \mathbb{N}$-re létezik n-nél nagyobb prímszám. Mivel $n!$ az $1, 2, \ldots, n$ számok mindegyikével osztható, ezért $N := n! + 1$ az $1, 2, \ldots, n$ számok mindegyikéhez relatív prím, tehát N nem osztható egyetlen n-nél kisebb prímmel sem. Vagyis N kanonikus alakjában kizárólag n-nél nagyobb prímek fordulnak elő. □

Tétel: Szomszédos összetett számokból tetszőlegesen hosszú sorozat létezik, azaz bármely $n \in \mathbb{N}$-re létezik olyan N, melyre az $N + 1, N + 2, \ldots, N + n$ számok mindegyike összetett.

Biz: Legyen $N := (n+1)! + 1$. Ekkor tetszőleges $2 \leq k \leq n+1$ esetén $k \mid (n+1)! + k = N + (k-1)$, tehát $N + 1, N + 2, \ldots, N + n$ egyaránt összetett. □

Def: Az a, b számok *ikerprímek*, ha prímek, és különbségük 2.

Megoldatlan probléma annak eldöntése, hogy véges vagy végtelen sok ikerprím van-e.

A prímek eloszlásáról szólnak a következő állítások.

Csebisev tétel: Tetszőleges n pozitív egészre létezik p prím, melyre $n < p < 2n$. □

Érdekesség, hogy a Csebisev tételre Erdős Pál találta az első elemi bizonyítást még középiskolás korában.

Dirichlet tétel: Ha $(a, d) = 1$ és $d > 0$, akkor az $a, a + d, a + 2d, \ldots$ végtelen számtani sorban végtelen sok prímszám található.

Prímszámtétel:

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1 \ ,$$

ahol ln az e alapú logaritmust, $\pi(x)$ pedig az x-nél nem nagyobb prímek számát jelöli. □

A prímszámokkal kapcsolatos megoldatlan problémák tárháza szinte kimeríthetetlen. Az egyik érdekes probléma a Goldbach sejtés, mely szerint minden 2-nél nagyobb páros szám előáll két prím összegeként. A Goldbach sejtésből egyébként közvetlenül következik a Csebisev tétel, hisz ha $n > 1$ és $2n + 2$ előáll két prím összegeként, mondjuk $2n + 2 = p + q$ alakban, akkor p és q közül a nagyobbik bizonyosan $n + 1$ és $2n - 1$ közé esik.

9. Kongruenciák

Def: [10] $a, b, m \in \mathbb{Z}$, $0 < m$ esetén azt mondjuk, hogy a *kongruens* b *modulo* m (jelölése $a \equiv b (\mathrm{mod}\ m)$, röviden $a \equiv b(m)$), ha $m \mid a - b$.

A fenti, m szerinti kongruencia ekvivalenciareláció, ugyanis (1) *reflexív*, azaz $a \equiv a(m)$, $\forall a \in \mathbb{Z}$, (2) *szimmetrikus*, azaz $a \equiv b(m) \Rightarrow b \equiv a(m)$, $\forall a, b \in \mathbb{Z}$, és (3) *tranzitív*, azaz $a \equiv b(m), b \equiv c(m) \Rightarrow a \equiv c(m)$, $\forall a, b, c \in \mathbb{Z}$. Ez azt jelenti, hogy az egész számok halmazát fel tudjuk bontani a modulo m kongruencia szerinti ekvivalenciaosztályokra, melyeket m *szerinti maradékosztályoknak* nevezünk. Két szám tehát akkor van azonos maradékosztályban, ha különbségük m többszöröse. Ezen a ponton még nem világos, hány maradékosztály is van modulo m. Inkább azt jegyezzük meg, hogy az m szerinti kongruencia kompatibilis a az összeadás, kivonás és szorzásműveletekkel:

Ha $a \equiv b(m)$ és $c \equiv d(m)$, akkor $a + c \equiv b + d(m)$ (hisz $m \mid a - b + c - d$), illetve $ac \equiv bd(m)$ (u.i. $m \mid a(c-d) + d(a-b) = ac - ab$), és innen látszik az is, hogy $a - c \equiv b + (-1)c \equiv b + (-1)d \equiv b - d(m)$.

[10] Aki szeretné, hogy a vizsgáztató alaposan kikérdezze tőle a kongruenciákat, használja a következő definíciót: $a \equiv b$ (mod m) azt jelenti, hogy a és b m-mel osztva ugyanannyi maradékot ad. Ekkor persze a következő természetes kérdés, hogy mit is jelent az osztási maradék. Nos, ezt lehetséges helyesen definiálni, és az alternatív definíció persze ekkor ekvivalens lesz az „igazival". Azonban az ebben a részben szereplő állítások nagy részének bizonyítása sokkal ügyetlenebb, ha ezt a definíciót használjuk, ráadásul egyúttal azt is jelezzük a vizsgáztatónak, hogy nagy valószínűséggel a maradékosztály fogalmát sem értjük pontosan. (Jegyezzük meg azért, hogy sokszor hasznos az alternatív definíció ismerete.)

A fenti kompatibilitás miatt, egy maradékosztályok vizsgálatakor elegendő csak a maradékosztályok reprezentánsait nézni, hisz modulo m kongruencia szempontjából (legalábbis az $+, -, \cdot$ műveletekre nézve) a maradékosztály elemei egyformán viselkednek. *Modulo m teljes maradékrendszernek* nevezzük tehát egész számok egy H halmazát, ha H minden modulo m maradékosztályból pontosan egy elemet tartalmaz, azaz, ha H bármely két, különböző h_1, h_2 elemére $h_1 \not\equiv h_2(m)$, továbbá tetszőleges $z \in \mathbb{Z}$ egészhez létezik $h \in H$, melyre $z \equiv h(m)$.

Állítás: Az m szerinti maradékosztályok száma m. Más szóval, ha H teljes maradékrendszer modulo m, akkor $|H| = m$.

Biz: Vegyük észre, hogy a $H = \{0, 1, \ldots, m-1\}$ teljes maradékrendszer modulo m, hiszen bármely két elemének különbsége m-nél kisebb, így H elemei különböző maradékosztálybeliek. Továbbá bármely z egész kongruens H valamely elemével, hisz z egyértelműen írható fel $z = mq + r$ alakban, ahol az r maradék 0 és $m-1$ közötti. □

Az m szerinti kongruenciareláció nem kompatibilis az osztás művelettel, azaz $a \equiv b(m)$-ből általában nem következik az $\frac{a}{c} \equiv \frac{b}{c}(m)$, hiszen lehet, hogy $\frac{a}{c}$ egész, $\frac{b}{c}$ pedig nem az.

Állítás: Ha $ad \equiv bd(m)$, akkor $a \equiv b(\frac{m}{(m,d)})$.

Biz: Legyen $D = (m, d)$ és $m = m'D$, ill. $d = d'D$. Ekkor $m'D = m \mid ad - bd = (a-b)d = (a-b)Dd'$, ezért $m' \mid d'(a-b)$. Mivel a d' kanonikus alakjában szereplő prímek nem szerepelnek m' kanonikus alakjában, ezért $m' \mid a - b$ következik, azaz $a \equiv b(m')$. □

Köv.: Ha $(m, d) = 1$ és $ad \equiv bd(m)$, akkor $a \equiv b(m)$. □

Egy teljes maradékrendszer segítségével könnyen kaphatunk egy másik teljes maradékrendszert.

Állítás: Legyenek k és $m \neq 0$ egészek, ill. $(a, m) = 1$. Ha H teljes maradékrendszer modulo m akkor $\{h + k : h \in H\}$ és $\{ah : h \in H\}$ egyaránt teljes maradékrendszerek modulo m. Azaz, ha egy teljes maradékrendszer minden eleméhez ugyanannyit adunk hozzá, vagy egy teljes maradékrendszert egy modulushoz relatív prím számmal végigszorzunk, akkor újfent teljes maradékrendszert kapunk.

Biz: Mivel mindkét vizsgált rendszer mérete m, csupán azt kell ellenőrizni, hogy mindkét rendszerre igaz, hogy elemei páronként különböző maradékosztályba tartoznak modulo m. Tehát, ha $h_1 + k \equiv h_2 + k(m)$ valamely $h_1, h_2 \in H$ esetén, akkor $h_1 \equiv h_2(m)$ a kivonás kompatibilitása miatt, és ezért $h_1 = h_2$, hisz H teljes maradékrendszer. Másfelől, ha $ah_1 \equiv ah_2(m)$, akkor $(a, h) = 1$ miatt lehet osztani, vagyis $h_1 \equiv h_2(m)$ és ismét $h_1 = h_2$ következik. Tehát mindkét halmaz valóban teljes maradékrendszer. □

Láttuk, hogy osztani csak a modulushoz relatív prím számmal lehet a modulus megváltozása nélkül. Ha azonban olyan osztóval akarunk osztani, mely az egyik oldalt nem osztja (pl az $5x \equiv 3(11)$ kongruenciát akarjuk x-re megoldani, ezért 5-tel szeretnénk osztani), akkor a fenti, osztással kapcsolatos megfigyelések nem segítenek. Ha azonban ilyen esetben az osztást a reciprokkal való szorzásnak tekintjük, akkor csupán arra van szükség, hogy —az előbbi példánál maradva— meghatározzuk az 5 reciprokát modulo 11, és azzal szorozzunk. A továbbiakban ez a cél vezet bennünket.

Megfigyelés: Ha $(a, m) = 1$ és $a \equiv b(m)$, akkor $(b, m) = 1$.

Biz: Mivel $m \mid a - b$, ezért minden $d \mid m$ esetén $d \mid a \iff d \mid b$. □

A fenti megfigyelés szerint, ha egy a szám relatív prím m-hez, akkor a maradékosztályának minden eleme relatív prím m-hez. Vagyis modulo m kétféle maradékosztály létezik: az egyiknek minden eleme relatív prím m-hez (ezek a *relatív prím maradékosztályok*), a másik fajtabeliek minden elemének van 1-nél nagyobb közös osztója m-mel.

Def: A $H \subset \mathbb{Z}$ halmaz *redukált maradékrendszer modulo m*, ha H minden olyan modulo m maradékosztályból, melyek elemei relatív prímek m-hez pontosan egy elemet tartalmaz. Azaz, H minden h elemére $(h, m) = 1$, továbbá, minden a egészhez, melyre $(a, m) = 1$ egyértelműen létezik $h \in H$ úgy, hogy $a \equiv h(m)$. Az m szerinti redukált maradékrendszer elemszámát (vagyis az m-hez relatív prím maradékosztályok számát) $\varphi(m)$ jelöli.

Redukált maradékrendszert kapunk pl. akkor, ha egy teljes maradékrendszerből elhagyjuk a modulushoz nem relatív prím elemeket. Így $\varphi(m)$ definiálható úgy is, mint az $1, 2, \ldots, m-1$ számok közül az m-hez relatív prímek száma. (Itt a $0, 1, \ldots, m-1$ teljes maradékrendszerből indultunk ki.)

A relatív prím maradékosztályok fontos tulajdonsága, hogy két ilyen maradékosztály szorzata is relatív prím maradékosztály lesz. Ennél több is igaz.

Állítás: Ha $(a, m) = 1$, és $H = \{h_1, h_2, \ldots, h_{\varphi(m)}\}$ pedig egy redukált maradékrendszer modulo m, akkor $aH := \{ah_1, ah_2, \ldots, ah_{\varphi(m)}\}$ is redukált maradékrendszer modulo m.

Biz: Azt kell igazolni, hogy az ah_i-k páronként különböző, m-hez relatív prím maradékosztályokhoz tartoznak, hisz ekkor szükségképpen minden relatív prím maradékosztályból pontosan egy reprezentáns szerepel. Minden ah_i relatív prím maradékosztályba tartozik, mert m-nek sem a-val, sem h_i-vel nincs közös prímosztója, így $(m, ah_i) = 1$. E maradékosztályok pedig különbözőek, hiszen ha $ah_i \equiv ah_j(m)$,

akkor a-val oszthatunk az osztásról szóló következmény szerint, azaz $a_i \equiv a_j(m)$, ahonnan $i = j$ következik. □

A fenti állításból következik a kongruenciák elméletének egyik legfontosabb tétele, mellyel meghatározható a korábban hivatkozott modulo m reciprok.

Euler-Fermat tétel: Ha $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1(m)$.

Biz: Legyen $H = \{h_1, h_2, \dots h_{\varphi(m)}\}$ redukált maradékrendszer modulo m. Az előző megfigyelés szerint az a-val végigszorzott $aH := \{ah_1, ah_2, \dots ah_{\varphi(m)}\}$ is redukált maradékrendszer modulo m. A szorzás kompatibilitása miatt $\prod_i h_i \equiv \prod_i ah_i(m)$, ami azt jelenti, hogy $\prod_i h_i \equiv a^{\varphi(m)} \prod_i h_i(m)$. Mivel $(m, \prod_i h_i) = 1$, az osztásra vonatkozó megfigyelés szerint $a^{\varphi(m)} \equiv 1(m)$, amit bizonyítani akartunk. □

Köv.: (kis Fermat tétel) Ha p prím, akkor bármely a egészre $a^p \equiv a(p)$.

Biz: Világos, hogy $\varphi(p) = p - 1$ (hisz 1-től $p - 1$-ig minden egész relatív prím p-hez), ezért ha $(a, m) = 1$, akkor $a^{p-1} \equiv 1(p)$, ahonnan $a^p \equiv a(p)$. Ha $(a, p) \neq 1$, akkor p prímtulajdonsága miatt $p \mid a$, azaz $a \equiv 0(p)$, és $a^p \equiv 0 \equiv a(p)$. □

A fenti bizonyításban láttuk, hogy $\varphi(p) = p - 1$, ha p prím. Ahhoz, hogy az Euler-Fermat tételt valóban használni tudjuk, jó ha ki tudjuk számítani $\varphi(m)$-t tetszőleges m modulusra. Prímhatványmodulusra könnyű dolgunk van: ha $n = p^\alpha$ valamely p prímre, akkor a és n pontosan akkor *nem* relatív prímek ha $p \mid a$. Tehát $\varphi(n)$ nem más, mint az 1 és n közötti, p-vel nem osztható egészek száma. Mivel a p-vel oszthatóak száma $\frac{n}{p} = p^{\alpha-1}$, így $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = (1 - \frac{1}{p})n$.

A célunk $\varphi(n)$ kiszámítása n kanonikus alakjából. Ehhez a kulcs a φ számelméleti függvény ú.n. multiplikatív tulajdonsága. Nem tilos ezt a tulajdonságot a szita-formulával bizonyítani, de mi próbálunk egy szemléletesebb utat követni.

Tétel: Ha $(m, n) = 1$ akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

Biz: Azt kell meghatároznunk, hogy a $H = \{1, 2, \dots, mn\}$ halmazban hány mn-hez relatív prím szám van. Egy a szám pontosan akkor relatív prím mn-hez, ha a m-hez is és n-hez is relatív prím. A kérdés tehát úgy is fogalmazható, hogy a H halmazban n-hez relatív prímek között hány szám relatív prím m-hez.

Tekintsünk egy $m \times n$ méretű mátrixot, melynek tehát m sora és n oszlopa van. Töltsük ki a mátrixot a H halmaz elemeivel, azaz írjuk be az első sorba az $1, 2, \dots, n$, a másodikba az $n+1, n+2, \dots, 2n$, stb, általában az i-dik sorba az $(i-1)n+1, (i-1)n+2, \dots, in$ számokat. Az ilyen módon kitöltött táblázat j-dik oszlopában a $j, n+j, 2n+j, \dots, (m-1)n+j$ számok állnak. Vegyük észre, hogy ezek a számok egyfelől modulo n azonos maradékosztályból kerülnek ki, másrészt pedig modulo m egy teljes maradékrendszert alkotnak. Az utóbbi állítás azért igaz, mert a j-dik oszlopot úgy kapjuk a $0, 1, 2, \dots, m-1$ (modulo m) teljes maradékrendszerből, hogy minden elemet végigszorzunk az m-hez relatív prím n számmal, majd megnöveljük j-vel. Egy korábbi állításban láttuk, hogy ezáltal teljes maradékrendszert kapunk modulo m.

Hol helyezkednek tehát el a táblázatban az n-hez relatív prím számok? Világos, hogy ezek a táblázatnak éppen $\varphi(n)$ oszlopát alkotják. Minden egyes ilyen oszlop egy teljes maradékrendszer modulo m, ezért minden egyes oszlopban $\varphi(m)$ olyan szám áll, ami m-hez is relatív prím. A táblázatban tehát az mn-hez relatív prím számok $\varphi(n)$ oszlop mindegyikében $\varphi(m)$ mezőt töltenek ki. Vagyis $\varphi(mn) = \varphi(m) \cdot \varphi(n)$, és éppen ezt akartuk bizonyítani. □

Köv.: Ha $n = \prod_{i=1}^k p_i^{\alpha_i}$ az n kanonikus alakja, akkor

$$\varphi(n) = \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \cdot \prod_{p \mid n,\ \text{prím}} (1 - \frac{1}{p}) \ .$$

Biz: A multiplikativitásról szóló tétel szrint $\varphi(n) = \varphi(\prod_{i=1}^k p_i^{\alpha_i}) = \varphi(p_1^{\alpha_1}) \cdot (\prod_{i=2}^k p_i^{\alpha_i}) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \ (\prod_{i=3}^k p_i^{\alpha_i}) = \dots = \prod_{i=1}^k \varphi(p_i^{\alpha_i}) = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$, ill. $\prod_{i=1}^k \varphi(p_i^{\alpha_i}) = \prod_{i=1}^k p_i^{\alpha_i} \cdot (1 - \frac{1}{p}) = \left(\prod_{i=1}^k p_i^{\alpha_i}\right) \cdot \left(\prod_{i=1}^k (1 - \frac{1}{p})\right) = n \cdot \prod_{i=1}^k (1 - \frac{1}{p})$. □

Wilson tétel: Ha p prím, akkor $(p-1)! \equiv -1(p)$.

Biz: Minden $1 \leq a \leq p-1$ egészhez tartozik egy $1 \leq b \leq p-1$ egész, melyre $ab \equiv 1(p)$, nevezetesen az a b, melyre $b \equiv a^{p-2}(p)$, hiszen ekkor valóban $ab \equiv a^{p-1} \equiv 1(p)$. Könnyen látható, hogy ha a-hoz b tartozik, akkor b-hez a tartozik, ugyanis a b-hez tartozó szám $b^{p-2} \equiv (a^{p-2})^{p-2} = a^{p^2-4p+4} = (a^{p-1})^{p-3} \cdot a \equiv 1^{p-3} \cdot a \equiv a(p)$. Rendezzük át a $(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1)$ tényezőit úgy, hogy párosával álljanak a fenti értelemben egymáshoz tartozó számok. Ekkor minden pár szorzata 1 lesz modulo p, de lesznek olyan számok is, melyek nem állnak párban, mert saját maguk reciprokai. Ezekre az a számokra $a^{p-2} \equiv a \equiv a^p(p)$ teljesül, azaz $a^2 \equiv 1(p)$, ami azt jelenti, hogy $p \mid a^2 - 1 = (a+1)(a-1)$, vagyis $a = 1$ vagy $a = p-1$. Tehát $(p-1)! \equiv 1 \cdot (p-1) \equiv -1(p)$, győztünk. □

Ha általában szeretnénk tudni, milyen maradékot ad $(n-1)!$ n-nel osztva, akkor ezt összetett n-ekre is könnyen megkaphatjuk. Ha n felbontható két különböző nemtriviális a és b osztójának szorzatára, akkor $n = ab \mid (n-1)!$ miatt $(n-1)! \equiv 0(n)$. Ha n nem ilyen összetett szám, akkor n egy p prím négyzete, de ekkor $p > 2$ esetén $n \mid p \cdot 2p \mid (n-1)!$ miatt szintén $(n-1)! \equiv 0(n)$ adódik, míg a kimaradó egyetlen eset a $p = 2$, amikoris $n = 4$, és $(n-1)! \equiv 2(n)$.

Rátérünk ezek után a lineáris kongruenciák tárgyalására. *Lineáris kongruencián* egy $ax \equiv b(m)$ kongruenciát értünk, ahol a és b adott egészek, m pedig adott pozitív egész. (Az $m = 1$ eset nem túl izgalmas, általában $m \geq 2$-vel fogunk foglalkozni.) A *lineáris kongruencia megoldása* azt jelenti, hogy meghatározzuk mindazon egészeket, melyeket x helyébe írva a kongruencia igaz lesz.

Amikor kongruenciákkal dolgozunk, akkor általában úgy végzünk műveleteket, hogy mindkét oldalon ugyanazzal a számmal végezzük az adott műveletet. Összefoglaljuk a kongruenciákkal végezhető műveletekkel kapcsolatos legfontosabb tudnivalókat.

Tétel: (1) $a \equiv b(m) \iff a + k \equiv b + k(m)$, (2) $a \equiv b(m) \Rightarrow ad \equiv bd(m)$,
(3) $ad \equiv bd(m) \iff a \equiv b(\frac{m}{(m,d)})$, (4) így $(m,d) = 1$ esetén $(a \equiv b(m) \iff ad \equiv bd(m))$ □

Tehát az összeadás és kivonás ekvivalens átalakítások, a szorzás ill. osztás csak akkor, ha a szorzó ill. osztó a modulushoz relatív prím. Egyébként a modulust is szorozni, ill. osztani kell, hogy az ekvivalencia megmaradjon. Az alábbi tétel a megoldható lineáris kongruenciákat jellemzi.

Tétel: Az $ax \equiv b(m)$ kongruencia pontosan akkor oldható meg, ha $(a,m) \mid b$. Ha ez teljesül, akkor a kongruencia megoldáshalmaza (a,m) darab maradékosztály modulo m.

Biz: Legyen $d := (a,m)$. Ha az $ax \equiv b(m)$ kongruencia megoldható, akkor $d \mid m \mid ax-b$, így $d \mid a \mid ax$ miatt $d \mid b$ következik. Ezzel a szükségességet igazoltuk.

Tegyük fel tehát, hogy $d \mid b$. A d-vel való osztást a fentiek szerinti ekvivalens átalakításként elvégezve az $a'x \equiv b'(m')$ kongruencia adódik, ahol $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ ill. $m' \equiv \frac{m}{d}$. Mivel a lnko-val osztottunk, $(a', m') = 1$, ezért a kongruencia mindkét oldalának megszorzása az m'-höz relatív prím $a^{\varphi(m')-1}$-gyel ekvivalens átalakítás, tehát a kongruenciánk $x \equiv a^{\varphi(m')}x = a^{\varphi(m')-1} \cdot ax \equiv a^{\varphi(m')-1}b(m)$ alakot ölt, tehát pontosan azon x-ek teszik igazzá a nyitott mondatot, melyekre $x \equiv a^{\varphi(m')-1}b(m')$.

Azt kaptuk, hogy a megoldások halmaza pontosan egy maradékosztály modulo m'. Hátra van még, hogy a megoldásokat modulo m adjuk meg. Minthogy $m = m'd$, ezért minden m'-maradékosztály pontosan d darab m-maradékosztály uniója, a konkrét esetben az alábbi reprezentánsokkal írható fel a megoldás: $x \equiv a^{\varphi(m')-1}b(m)$, vagy $x \equiv a^{\varphi(m')-1}b + m'(m)$, vagy $x \equiv a^{\varphi(m')-1}b + 2m'(m)$, vagy ..., vagy $x \equiv a^{\varphi(m')-1}b + (d-1)m'(m)$. □

Sokszor szükség van a lineáris kongruenciák gyakorlatban történő megoldására. A fenti bizonyításban vázolt módszert első lépése, az (a,m)-val való leosztás minden további nélkül végrehajtható (pl. az Euklideszi algoritmust alkalmazva), azonban a továbbiak elvégzéséhez ismerni kell $\varphi(m')$-t. Ezt azonban nem tudjuk kiszámítani m' kanonikus alakja nélkül, ami nem feltétlenül áll rendelkezésre. Tehát ha már elértük, hogy az $ax \equiv b(m)$ lineáris kongruenciában $(a,m) = 1$, akkor a kongruenciát visszavezethetjük egy kisebb modulusú kongruenciára. Feltehető ugyanis, hogy $0 \leq a < m$. Mivel a kongruencia ekvivalens azzal, hogy

$$ax - b = mx_1 \quad , \qquad \text{ahonnan} \qquad x = \frac{mx_1 + b}{a}$$

valamely x_1 egészre. Elegendő tehát megoldani az $mx_1 \equiv -b(a)$ kongruenciát, és a kapott x_1-t visszahelyettesíteni az x-t megadó (második) egyenletbe. Ezáltal az eredeti kongruenciát visszavezettük egy a-modulusú kongruenciára. Az eljárást követve, előbb-utóbb egy $x_i \equiv c'(m')$ kongruencia adódik, ahonnan $x_i = m' \cdot n + c'$, és ezt visszahelyettesítgetve x-t végül fel tudjuk írni $x = mn + c$ alakban, vagyis $x \equiv c(m)$ lesz a megoldás.

Sokszor célravezető módszer lehet ügyes szorzásokkal elvégzett ekvivalens átalakítások egymásutánja is. Ilyenkor a modulus végig m marad, de a cél rendszerint $|a|$ csökkentése, egészen $|a| = 1$-ig, majd esetleges -1-gyel való szorzás adja a végeredményt. Amennyiben a lineáris kongruenciában kis számok szerepelnek, ez a leggyorsabb eljárás a megoldásra. A módszert itt nem részletezzük, a gyakorlatokon az érdeklődő olvasó nyilván számos példát látott a lineáris kongruencia „ügyeskedéssel" történő megoldására. Megjegyezzük azonban, hogy a vizsgán számítani kell arra, hogy egy „véletlen" kongruenciát a vizsgáztató előtt kell megoldania a hallgatónak.

10. Algebrai struktúrák

Def: A H *halmazon értelmezett n-változós művelet*en egy tetszőleges $f : H^n \to H$ leképezést értünk, azaz minden, H elemeiből képzett rendezett n-eshez (pl. $(h_1, h_2, \ldots, h_n)$-hez) H-nak egy bizonyos elemét

(itt $f(h_1, h_2, \ldots, h_n)$-t) rendeljük.

Megjegyzés: Rendszerint kétváltozós műveletekkel fogunk foglalkozni. Ilyen esetben a művelet jelét az összeművelt elemek közé (és nem elé) írjuk, azaz nem $+(2,2)$-ről, hanem $2+2$-ről beszélünk. Ez a konvenció a továbbiakban nem fog felreértést okozni. (Valószínűleg az volna csak igazán zavaró, ha nem alkalmaznánk ezt a konvenciót: tessék csak kiértékelni a $\cdot(-(+(3,2),1),\cdot(2,2))$ kifejezést!)

Példa: Kétváltozós művelet pl. a valós számokon az összeadás, a szorzás, vagy éppen a kivonás. A pozitív számokon az osztás és a hatványozás. Egyváltozós műveletnek tekinthető pl. az ellentett képzése a racionális számok halmazán (x-hez $-x$-t rendelünk) vagy a pozitív számokon a reciprok képzése. Nullaváltozós művelet pl. az egészeken az, hogy 5. Háromváltozós művelet a valós számokon amely az x, y, z számokhoz $x(y+z) + \frac{\log|x^3+1|}{y^2+1}$-t rendel. Kétváltozós művelet vektortérben a vektorösszeadás vagy egy vektortér lineáris leképezéseinek kompozíciója (egymásutánja), utóbbi esetben $Hom(V,V)$ az alaphalmaz. A valós polinomokon kétváltozós művelet az összeadás vagy a kompozíció (ami itt behelyettesítést jelent). Egyváltozós művelet a polinomokon deriválás, vagy a $[0,x]$ intervallumon történő integrálás.

Nem művelet (a most használt értelemben) a hatványozás a valós számokon, mert $(-1)^{\frac{1}{2}} = \sqrt{-1}$ nem valós szám. Nem művelet a valós számokon az osztás sem, mert a $\frac{0}{0}$ nem valós szám. Szintén nem művelet a skalárral való szorzás vektotereken, mert a két összeművelendő elem nem azonos halmazból kerül ki.

Def: Az $\mathcal{S} = \langle H, \{f_i : i \in I\}\rangle$ egy *algebrai struktúra*, ha minden $i \in I$-re f_i a H halmazon értelmezett (mondjuk n_i-változós) művelet.

Példa: Algebrai struktúra a valós számok halmaza az összeadásra és kivonásra ($\langle \mathbb{R}, \{+,-\}\rangle$). Szintén algebrai struktúra a pozitív számok halmaza a szorzásra, mint kétváltozós műveletre nézve, de algebrai struktúra $\langle \mathbb{R}, +\rangle$ is. Utóbbi két algebrai struktúra „lényegében" azonos, u.i. $\log xy = \log x + \log y$, azaz a pozitív számok szorzásra pontosan úgy viselkednek, mint a logaritmusaik az összeadásra. Erről szól a következő definíció.

Def: Az $\mathcal{S} = \langle H, \{f_i : i \in I\}\rangle$ és az $\mathcal{S}' = \langle H', \{f'_i : i \in I\}\rangle$ algebrai struktúrák *izomorfak*, ha az f_i és f'_i műveletek tetszőleges $i \in I$ esetén ugyanannyi (mondjuk n_i) változósak, továbbá létezik egy $\varphi : H \to H'$ bijekció, melyre $\varphi(f_i(h_1, h_2, \ldots, h_{n_i})) = f'_i(\varphi(h_1), \varphi(h_2), \ldots, \varphi(n_{n_i}))$ tetszőleges $i \in I$ és $h_1, h_2, \ldots, h_{n_i} \in H$ esetén. (Vagyis a leképezés *művelettartó*: az összeművelt elemek képét úgy kapjuk, hogy összeműveljük a képeket.)

Példa: Vektorterek korábban megismert izomorfizmusa egy speciális izomorfia a két összeadásművelettel ellátott algebrai struktúra között. A specialitás abból adódik, hogy a skalárral való szorzásra (ami ugyebár nem *algebrai* értelemben vett művelet) szintén megkívánjuk a „művelettartást".

Def: Tegyük fel, hogy $\mathcal{S} = \langle H, \{f_i : i \in I\}\rangle$ egy algebrai struktúra, és a $H' \subset H$ halmaz olyan, hogy egyetlen f_i művelet sem vezet ki belőle (azaz $f_i(h_1, h_2, \ldots, h_{n_i}) \in H'$ ha $h_1, h_2, \ldots, h_{n_i} \in H'$). Ekkor az $\mathcal{S}' = \langle H', \{f_i|_{H'} : i \in I\}\rangle$ algebrai struktúrát az $\mathcal{S}$ struktúra *részstruktúrának* nevezzük, és ezt a tényt $\mathcal{S}' \leq \mathcal{S}$-sel jelöljük. ($f_i|_{H'}$ az f_i művelet H'-re megszorított változatát jelenti. A továbbiakban a megszorítás jelölését mellőzzük, ha ez nem okoz féreértést.)

Példa: $\langle \mathbb{N}, \{+,\cdot\}\rangle \leq \langle \mathbb{R}, \{+,\cdot\}\rangle$. Ha V vektortér, és U egy altere, akkor $\langle U, +\rangle \leq \langle V, +\rangle$.

Megfigyelés: Ha az $\mathcal{S}_j = \langle H_j, \{f_i : i \in I\}\rangle$ struktúra minden $j \in J$-re az $\mathcal{S} = \langle H, \{f_i : i \in I\}\rangle$ struktúra részstruktúrája, akkor a $\bigcap_{j\in J} \mathcal{S}_j := \langle \bigcap_{j\in J} H_j, \{f_i : i \in I\}\rangle$ metszetstruktúra is részstruktúrája az $\mathcal{S}$ algebrai struktúrának.

Biz: Csak azt kell ellenőrizni, hogy az f_i-k megszorításai műveletek, azaz nem vezetnek ki a metszetből. Ám mivel egyik H_j-ből sem vezetnek ki, azért a metszetből sem. □

Def: Legyen $\mathcal{S} := \langle H, \{f_i : i \in I\}\rangle$ egy algebrai struktúra, és a $K \subset H$. A K *által generált* $\langle K\rangle$ *részstruktúra* a legszűkebb olyan részstruktúrája $\mathcal{S}$-nek, mely K-t tartalmazza, azaz $\langle K\rangle := \bigcap_{K\subset\mathcal{S}'\leq\mathcal{S}} \mathcal{S}'$.

10.1. Csoportok

Láttuk, hogy a műveletekre nincs más megkötés azon túl, hogy ne vezessenek ki az adott struktúrából, így nem is várható, hogy jól használható, mély tételeket kapjunk egy ennyire általános definícióból. Célszerű tehát további megkötéseket tenni a vizsgált struktúrákra. Erre a legtermészetesebb mód, hogy a művelet(ek)től különböző tulajdonságokat várunk el.

Def: A H halmazon értelmezett, 2-változós $\star$ művelet *asszociatív* (magyarul *átzárójelezhető*), ha tetszőleges $x, y, z \in H$ elemekre $x \star (y \star z) = (x \star y) \star z$ áll. A $\star$ művelet *kommutatív* (magyarul *felcserélhető*), ha tetszőleges $x, y \in H$ elemekre $x \star y = y \star x$ teljesül.

Példa: A vektorterekben értelmezett + művelet asszociatív és kommutatív, a pozitív számokon értelmezett hatványozás nem asszociatív és nem kommutatív, az $n \times n$-es mátrixok szorzása asszociatív,

de nem kommutatív, míg a valós számokon értelmezett *számtani közép* művelet kommutatív, de nem asszociatív.

Def: Az $\mathcal{S} = \langle H, \star \rangle$ struktúra *félcsoport*, ha $\star$ a H-n asszociatív. Ha $\star$ kommutatív is, akkor $\mathcal{S}$ *Abel félcsoport*.

Példa: Láttuk, hogy az $n \times n$-es mátrixok a szorzásra félcsoportot alkotnak. Az $n \times n$-es, szimmetrikus mátrixok e félcsoportnak egy Abel részfélcsoportját alkotják.

Def: Legyen $\star$ kétváltozós művelet H-n. Az $e \in H$ elem az $\star$ művelet *egységeleme*, ha $e \star h = h \star e = h$ a H tetszőleges h elemére.

Megfigyelés: Ha az $\mathcal{S}$ struktúra $\star$ műveletének létezik egységeleme, akkor egyetlen egységeleme létezik.

Biz: Tegyük fel, hogy $e, e' \in H$ egyaránt egységelemek, ekkor $e = e \star e' = e'$. □

Def: Ha az $\mathcal{S} = (H, \star)$ struktúrában $e \in H$ a $\star$ művelet egységeleme, és $h \star h' = h' \star h = e$, akkor az mondjuk, hogy h' a h *inverze* a $\star$ műveletre. (Egyúttal h a h' inverze $\star$-ra nézve.)

Példa: Az $\langle \mathbb{R}, \{+, \cdot\} \rangle$ struktúrában az összeadás egységeleme a 0, az x elem inverze $-x$. A szorzás egységeleme az 1, az $x \neq 0$ elem inverze az $\frac{1}{x}$.

Def: A $\mathcal{S} = \langle G, \cdot \rangle$ struktúra *csoport*, ha (1) $\mathcal{S}$ félcsoport, (2) a $\cdot$ műveletnek létezik egységeleme, és (3) minden $g \in G$ elemnek létezik inverze a $\cdot$ műveletre. Ha a csoportműveletet $\cdot$ jelöli, és a megadáskor ennek elhagyása nem okoz félreértést, akkor a fenti csoportot egyszerűen G-vel jelöljük. Szorzásművelettel ellátott csoport esetén (a valós szorzásműveleti jelhez hasonlóan), ha nem okoz félreértést, elhagyjuk a műveleti jelet két elem összeművelésekor, azaz $g \cdot h$ helyett gyakran csak gh-t írunk. A szorzásművelettel ellátott csoportban beszélhetünk hatványozásról: egy g elem n-dik hatványa nem más, mint az elemet n-szer összeszorozzuk (helyesebben összeműveljük) önmagával. A 0-dik hatványt az egységelemként definiáljuk, a $(-n)$-dik hatvány pedig a g^{-1} inverzelem n-dik hatványa. A G csoport *rendje* $|G|$. A G csoport *Abel csoport*, ha G csoportművelete kommutatív.

Példa: $\langle \mathbb{R}, + \rangle, \langle \mathbb{Z}, + \rangle, \langle \mathbb{R} \setminus \{0\}, \cdot \rangle, \langle \mathbb{R}^{n \times k}, + \rangle$ Abel csoportok. Az $n \times n$-es reguláris mátrixok a szorzásra nézve (nemkommutatív) csoportot alkotnak[11].

Megfigyelés: Ha G csoport, akkor minden elemnek egyértelmű inverze van.

Biz: Ha x és y a g inverzei és e a G egységeleme, akkor $x = xe = x(gy) = (xg)y = ey = y$. □

Az algebrai struktúrákról elmondottak csoportokra vonatkozó közvetelen következményeit foglaljuk össze az alábbiakban.

Köv.: (1) Két csoport *izomorf*, ha van köztük művelettartó bijekció.
(2) A *részcsoport* olyan részhalmaz, mely maga is csoport a csoportműveletre.
(3) Bármely G csoport tetszőleges részcsoportjainak metszete is G részcsoportja.
(4) A $K \subseteq G$ részhalmaz által *generált* $\langle K \rangle$ *csoport* a G csoport K-t tartalmazó részcsoportjainak metszete. □

10.2. Ciklikus csoportok

Def: Az olyan csoportot, melyet valamely eleme generál, *ciklikus csoport*nak nevezzük.
A G csoport g elemének *rendje* a g által generált részcsoport elemszáma.

Az elem rendjének definíciója úgy is kimondható, hogy a g elem rendje az a legkisebb n szám, melyre $g^n = e$. Ha ugyanis létezik ilyen n, akkor, $g^{-1} = g^{n-1}$, és a $g, g^2, g^3, \ldots, g^n$ elemek különbözőek (hisz ha $g^i = g^j$, akkor $g^{i-j} = e$), ezért $\langle g \rangle$ n-elemű. Ha pedig nem létezik olyen n, amire $g^n = e$ áll, akkor a $g, g^2, g^3, \ldots$ elemek mind különbözőek, ezért $\langle g \rangle$ végtelen.

Ha $\langle G, \cdot \rangle$ ciklikus csoport, melyet $g \in G$ generál, akkor G minden eleme előáll $g^i (= g \cdot g \cdot \ldots \cdot g$ [i-szer]) alakban, ahol $i \in \mathbb{Z}$. Ha G rendje véges, akkor elegendő a pozitív i kitevőkre szorítkozni. Ha G végtelen, akkor a generátorelemnek semelyik hatványa sem egységelem, mert egyébként a generátorelem csak véges sok elemet generálna.

Hányfélék lehetnek a ciklikus csoportok, azaz izomorfia erejéig hogy néznek ki a ciklikus csoportok? Nyilvánvaló, hogy ha két ciklikus csoport rendje különböző, akkor nem izomorfak. Ha azonban $|G| = |H| = n$ a G és H ciklikus csoportra, akkor $G \cong H$. Legyen ugyanis g ill. h a G ill H generátoreleme. Ekkor g^n ill. h^n a G ill. H egységeleme, a két csoport minden eleme g^i ill. h^i alakú, és könnyen látható, hogy $\varphi(g^i) := h^i$ izomorfizmus. Tehát a véges ciklikus csoportot az elemszáma (izomorfia erejéig) meghatározza. Az n-elemű ciklikus csoportot C_n jelöli, és könnyen látható, hogy $C_n \cong \mathbb{Z}_n$, ahol $\mathbb{Z}_n$ a $\langle \mathbb{Z}_n, + \rangle$ csoportot jelöli, ahol $\mathbb{Z}_n$ a modulo n maradékosztályok halmaza. Minden véges ciklikus

[11] Az egységelem itt az $n \times n$-es egységmátrix, az inverz pedig az adott mátrix inverze. (Ugyebár egy mátrix akkor reguláris, ha létezik inverze, és arra is emlékezhetünk éppenséggel, hogy egy mátrix pontosan akkor reguláris, ha determinánsa nem nulla, így (a determinánsok szorzástétele miatt) reguláris mátrixok szorzata reguláris.)

csoportot leírtunk tehát. Ha G végtelen ciklikus csoport, akkor a g generátorelem semelyik hatványa sem egységelem, mert egyébként g véges csoportot generálna. Mivel a g hatványai egy H részcsoportot alkotnak, ezért $H = \langle g \rangle = G$, ez a részcsoport maga a csoport. Azt kaptuk tehát, hogy minden végtelen, ciklikus csoport a $\langle \mathbb{Z}, + \rangle$ csoporttal izomorf.

Tétel: Ciklikus csoport minden részcsoportja ciklikus.

Biz: Legyen a G ciklikus csoport egy generátoreleme g, és legyen $H \leq G$ részcsoport. Tekintsük a minimális $0 < k$-t, melyre $g^k \in H$ (ilyen létezik, ha H nem a triviális, egyelemű csoport (ami persze ciklikus)). Megmutatjuk, hogy g^k generálja H-t, amiből azonnal adódik, hogy H ciklikus. Nyilván g^k generálja a e, g^{ik}, g^{-ik} elemeket tetszőleges pozitív egész i esetén. Tegyük fel, hogy a H részcsoport g^l elemét g^k nem generálja, azaz $k \nmid l$. Osszuk el l-t k-val maradékosan, azaz $l = ak+r$, ahol $1 \leq r < k$. Mivel $g^k, g^l \in H$, ezért $g^l \cdot ((g^k)^{-1})^a = g^{ak+l} \cdot g^{-ak} = g^{ak+r-ak} = g^r \in H$, ami ellentmond k választásának. Tehát H-t g^k csakugyan generálja, vagyis H valóban ciklikus. □

10.3. Diédercsoportok

Fontos példák csoportokra a szimmetriák alkotta csoportok. Legyen X egy halmaz, és tekintsük az $f : X \to X$ bijekcióknak egy olyan $\mathcal{F}$ nemüres halmazát, mely zárt a kompzícióra, vagyis $f, g \in \mathcal{F}$ esetén $f \circ g \in \mathcal{F}$, ahol $f \circ g(x) := f(g(x)) \ \forall x \in X$. Tegyük fel továbbá, hogy minden $f \in \mathcal{F}$ bijekció f^{-1} inverze is $\mathcal{F}$-ben van. Ekkor az $\mathcal{F}$ csoportot alkot a kompzíció műveletre, azaz $\langle \mathcal{F}, \circ \rangle$ csoport. A csoport egységeleme az id identikus (azaz a minden pontot helybenhagyó) leképezés (ez azért $\mathcal{F}$-beli, mert $id = f \circ f^{-1}$ tetszőleges $f \in \mathcal{F}$-re), a kompozícióra vonatkozó inverz az adott függvény inverze lesz, a kompozícióművelet asszociativitása pedig közvetlenül adódik a definícióból.

Az egyik legfontosabb példa a fenti szimmetriacsoportra a D_n *diédercsoport*, amikoris X a sík egy szabályos, n oldalú sokszöge, a bijekciók halmaza pedig az X sokszög egybevágóságainak halmaza (azaz a sík mindazon egybevágóságai, melyek az X sokszöget (mint halmazt) fixen hagyják). A D_n diédercsoport elemei tehát a szabályos n-szöget fixen hagyó egybevágóságok, a művelet pedig az egybevágóságok egymásutánja. Az egyik ilyen egybevágóság a sokszög középpontja körüli $\frac{2\pi}{n}$-szögű f forgatás, egy másik lehetséges egybevágóság a sokszög egy szimmetriatengelyére való t tükrözés. Lényeges tulajdonsága a diédercsoportnak, hogy $n > 2$-re nem kommutatív (u.i. $t \circ f \neq f \circ t$). Az f és t szimmetriák a sokszög minden szimmetriáját generálják, hiszen a körüljárástaró egybevágóságok középpont körüli forgatások, a körüljárásváltóak pedig úgy kaphatóak, hogy először tükrözünk, majd forgatunk.

A $t \circ t = id$, $f^n = f \circ f \circ \ldots \circ f[n\text{-szer}] = id$ ill. $f \circ t = t \circ f^{n-1} = t \circ f^{-1}$ azonosságok teljesülése egyszerűen ellenőrizhető. Ebből az látszik, hogy D_n minden eleme vagy f^k, vagy $t \circ f^k$ alakú valamely $0 \leq k < n$-re: ha ugyanis f és t is szerepel a kompzícióban, akkor a t-ket baloldalra csoportosíthatjuk a harmadik azonosság miatt.

10.4. Permutációcsoportok

Korábban már találkoztunk permutációkkal: a determináns definíciójában a permutáció inverziószáma volt érdekes, a leszámlálásoknál n elem lehetséges permutációinak számát vizsgáltuk, most pedig a permutációk struktúráját vesszük szemügyre. Emlékeztetünk, hogy a permutációk az $[n] := \{1, 2, \ldots, n\}$ halmaz bijekciói. Az $[n] \to [n]$ bijekciók zártak a kompozícióra és az inverzképzésre, ezért az $[n]$ halmaz permutációi szimmetriacsoportot alkotnak a kompozícióra.

Def: Az S_n *szimmetrikus csoport* az $[n]$ halmaz permutációi alkotta csoport a függvénykompozíció műveletre nézve.

A diédercsoportok után tehát a szimmetrikus csoport a második fontos példa a szimmetriacsoportra. Korábbi tanulmányainkat kamatoztatandó megfigyelhetjük, hogy az S_n szimmetrikus csoport rendje az $[n]$ permutációinak száma, vagyis $n!$. Láttuk, hogy a diédercsoport sem volt kommutatív, és mivel a D_n diédercsoport tekinthető a szabályos n-szög *csúcsain* ható permutációk egy halmazának, ezért $D_n \leq S_n$, így aztán S_n sem kommutatív $n > 2$-re.

A következő célunk a permutációk hatványait megvizsgálni, hogy konkrét permutációk rendjét meghatározhassuk. Legyen $i \in [n]$, $\sigma \in S_n$, és tekintsük az $i, \sigma(i), \sigma^2(i), \sigma^3(i), \ldots$ elemeket. Ezek az elemek (tehát azok, melyekbe a σ permutáció i-t elviszi) az i σ szerinti *orbitját* alkotják. σ bijektívitása miatt az orbitot alkotó sorozatban az elemek ciklikusan ismétlődnek, azaz $\sigma^{j+k}(i) = \sigma^j(i)$, ahol k az orbit mérete. Ha tehát leírjuk az $(i, \sigma(i), \sigma^2(i), \sigma^3(i), \ldots \sigma^{k-1}(i))$ elemeket, akkor i orbitjának minden egyes eleméről látjuk, hogy a σ a felsorolás következő elemébe viszi (az utolsót az elsőbe). Az fenti ciklikus sorrend a σ permutáció egy *ciklusa*. Mivel két elem orbitja vagy diszjunkt, vagy azonos, ezért igaz az alábbi megfigyelés.

Tétel: Minden permutáció felírható diszjunkt ciklusok szorzataként. □

A gyakorlatban is alkalmazzuk ezt a felírást, azaz ahelyett, hogy a σ permutációt az értelmezési tartomány minden elemén megadnánk, csupán egymás mellé írjuk a ciklusokat, melyek közül (ha n ismert) az egypontúakat (vagyis a fix

pontokat) kihagyjuk. Így pl a $\sigma = (1,7,4)(35) \in S_7$ permutációra $\sigma(4) = 1$ és $\sigma(2) = 2$. *Ciklikus permutáció*nak nevezünk egy permutációt, ha pontosan egy ciklusa van. Ha a σ permutációt hatványozzuk, akkor az elemek a ciklusukon belül mozognak, mégpedig minden elem kitevőnyit lép jobbra. Ebből látszik, hogyan lehet meghatározni σ legkisebb hatványát, mely minden elemet helyben hagy, vagyis azt a legisebb k kitevőt, melyre $\sigma^k = id$ az egységelem.

Tétel: Ha σ ciklusai $k_1, k_2, \ldots, k_l$ méretűek, akkor σ rendje a $k_1, k_2, \ldots k_l$ számok legkisebb közös többszöröse. □

*Transzpozíció*nak nevezzük az olyan permutációt, melynek egyetlen, kételemű ciklusa van, azaz a permutáció két elemet felcserél, a többit fixen hagyja.

Állítás: A tranzpozíciók generálják az S_n szimmetrikus csoportot.

Biz: Minden permutáció diszjunkt ciklusok szorzata, ezért elegendő megmutatni, hogy bármely ciklus előáll olyan transzpozíciók szorzataként, melyek csak a ciklus elemeit használják. Mivel az $(i_1, i_2, \ldots, i_k)$ ciklikus permutáció a $(i_1, i_k), (i_1, i_{k-1}), \ldots, (i_1, i_2)$ transzpozíciók szorzata, ezért az állítást igazoltuk. □

Értelmes kérdés, hogy legalább hány transzpozíció kell S_n generálásához. Minden transzpozíciónak megfelel egy él az $[n]$ ponthalmazon. Transzpozíciók egy halmazának tehát egy n-pontú gráf felel meg. Világos, hogy ha egy ilyen gráf nem összefüggő, akkor a szóbanforgó transzpozíciók nem generálják S_n-t, sőt: általában nem generálnak egyetlen olyan permutációt sem, mely a komponensek között (is) végez cserét. Tehát minden, transzpozíciókból álló generátorrendszernek összefüggő gráf felel meg, vagyis legalább $n-1$ transzpozíció kell S_n generálásához. Ennyi egyébként elegendő is: az $(1,2), (1,3), \ldots, (1,n)$ transzpozíciók alkalmas kompozíciójával tetszőleges S_n-beli permutáció előállítható. Egy adott σ permutáció pl. úgy konstruálható, hogy legfeljebb két transzpozíció kompozíciójával olyan σ_0 permutációt gyártunk, melyre $\sigma^{-1}(n) = \sigma_0^{-1}(n)$, majd σ_n-hez további transzpozíciókat komponálva olyan σ_1-t kapunk, melyre σ_1^{-1} és σ^{-1} az n és $n-1$ helyeken is megegyezik, s.í.t. Az i-dik lépésben σ_i kapjuk, melyre $\sigma_i^{-1}(k) = \sigma^{-1}(k)$ minden $k = n, n-1, n-2, \ldots n-i$-re. A σ_n permutációra $\sigma_n^{-1} = \sigma^{-1}$ áll, tehát a $\sigma = \sigma_n$ permutáció az említett transzpozíciók szorzata.

Def: Az S_n szimmetrikus csoport részcsoportjait *permutációcsoportnak* nevezzük.

Hányfélék lehetnek a permutációcsoportok? A válasz, hogy a permutációcsoportok (izomorfia erejéig) minden (véges) csoportot felölelnek.

Cayley tétel: Minden véges G csoport alkalmas permutációcsoporttal izomorf.

Biz: Az általánosság megszorítása nélkül feltehető, hogy G n-edrendű, és G elemei az $1, 2, \ldots, n$ számok. Ekkor G minden g elemének megfeleltethető egy σ_g permutáció az alábbiak szerint: $\sigma_g(i) := g \cdot i$. Ellenőrizzük, hogy a megfeleltetés homomorfizmus, azaz, hogy művelettartó: $\sigma_{gh} = \sigma_g \circ \sigma_h$. Csakugyan, tetszőleges $i \in [n]$ esetén $\sigma_{gh}(i) = (gh)i = g(hi) = g(\sigma_h(i)) = \sigma_g(\sigma_h(i)) = \sigma_g \circ \sigma_h(i)$. Az kell még, hogy a $g \mapsto \sigma_g$ leképezés injektív, azaz $g \neq h$ esetén $\sigma_g \neq \sigma_h$. De ez is igaz, mivel $\sigma_g(e) = ge = g \neq h = he = \sigma_h(e)$. Tehát a $\{\sigma_g : g \in G\}$ permutációk az S_n szimmetrikus csoport egy G-vel izomorf részcsoportját alkotják. □

Könnyen ellenőrizhető, hogy páros permutációk szorzata is páros permutáció, páros permutáció és páratlan permutáció szorzata páratlan permutáció, továbbá, hogy két páratlan permutáció szorzata pedig páros permutáció. Ez azt jelenti, hogy a páros permutációk az S_n szimmetrikus csoportnak egy részcsoportját alkotják. E részcsoport az A_n-nel jelölt *alternáló csoport*, rendje S_n rendjének fele, azaz $\frac{n!}{2}$.

10.5. A csoportelmélet alapjai

Def: A G csoport K és H részhalmazainak *komplexusszorzatán*

$$HK := \{hk : h \in H, k \in K\} \subseteq G$$

halmazt értjük. Ha $H \leq G$ és $g \in G$, akkor a gH (Hg) komplexusszorzat a H részcsoport *baloldali (jobboldali) mellékosztálya*. Ha $a \in gH$ ($a \in Hg$), akkor a-t a gH (Hg) mellékosztály *reprezentánsának* nevezzük.

Egy részcsoport mellékosztályainak figyelemreméltó struktúrája van.

Megfigyelés: Legyen $H \leq G \ni g, g'$. Ekkor (1) $g \in Hg$, (2) $g' \in Hg \Rightarrow Hg = Hg'$, (3) $Hg = Hg'$ vagy $Hg \cap Hg' = \emptyset$ (4) $|H| = |Hg|$

Biz: (1): $e \in H \Rightarrow g = eg \in Hg$.
(2): $g' = hg$ valamely $h \in H$-ra, ezért $Hg' = H(hg) = (Hh)g \subseteq Hg$. Mivel $g = h^{-1}g'$, ezért $g \in Hg'$, így az előző gondolatmenet szerint $Hg \subseteq Hg'$ is igaz.
(3): (2) miatt, ha $g^* \in Hg \cap Hg'$, akkor $Hg = Hg^* = Hg'$.
(4): Ha $h, h' \in H$ és $h \neq h'$, akkor $hg \neq h'g$, ezért a $h \mapsto hg$ bijekció H és Hg között. □

Köv.: (Lagrange tétel) Ha $H \leq G$, akkor $|H| \mid |G|$. Speciálisan, G bármely g elemének rendje (a g által generált részcsoport elemszáma) osztja G rendjét.

Biz: A G csoport néhány H szerinti (jobboldali) mellékosztály uniója, és minden mellékosztály $|H|$ elemet tartalmaz. □

Def: A $H \leq G$ részcsoport *indexe* a $|G|$ és $|H|$ hányadosa, jele $|G : H|$.

Köv.: Minden prímrendű csoport ciklikus.

Biz: Bármely, $e \neq g \in G$ elem a Lagrange tétel miatt kénytelen az egész csoportot generálni. □

Köv.: Ha G csoport, akkor bármely $g \in G$ rendje a G rendjének osztója.

Biz: A g elem rendje a $\langle g \rangle$ részcsoport rendje, mely a Lagrange tétel miatt $|G|$ osztója. □

Megjegyzés: Belátható, hogy a modulo m redukált maradékosztályok (tehát az n-hez relatív prím számok alkotta maradékosztályok) a szorzásra nézve csoportot alkotnak: a szorzás ugyanis művelet, mert m-hez relatív prímek szorzata relatív prím m-hez, és az m-mel vett maradéka csak a tényezők maradékától függ; az asszociativitás világos; az egységelem az 1-t tartalmazó maradékosztály; végül inverz azért létezik, mert az $ax \equiv b \pmod{n}$ kongruencia $(a,m) = 1$ esetén megoldható. Ha az utóbbi következményt alkalmazzuk erre a csoportra, akkor azt kapjuk, hogy tetszőleges a elem rendje osztója a csoport rendjének, azaz $\varphi(m)$-nek. Ez azt jelenti, hogy tetszőleges a elem $\varphi(m)$-dik hatványa az egységelemet adja, azaz ha $(a,m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$ teljesül. Az Euler-Fermat tétel tehát speciális esete a Lagrange tételnek.

Láttuk tehát, hogy minden csoport előáll, mint tetszőleges részcsoportja jobboldali mellékosztályainak diszjunkt uniója. Természetesen ugyanez a baloldali mellékosztályokra is igaz, azonban *általában* nem igaz, hogy ez a két előállítás azonos. Ha pl. a G csoport Abel, és $H \leq G$ részcsoport, akkor a kommutativitás miatt $Hg = gH$ a G minden g elemére, így ilyenkor a két felbontás valóban megegyezik. Ugyanez a szituáció nemkommutatív csoportokban is előfordul, és az ezt megvalósító részcsoportok különösen érdekesek.

Def: A G csoport N részcsoportja a G *normálosztója* (jelölése $N \trianglelefteq G$), ha $Ng = gN$ a G minden g elemére.

Világos, hogy minden részcsoport egyszerre bal- és jobboldali mellékosztálya önmagának. Ha tehát egy csoport indexe 2, akkor a részcsoport komplementere egyúttal jobb- és baloldali mellékosztály is, azaz minden 2 indexű részcsoport szükségképpen normálosztó. Például $A_n \trianglelefteq S_n$. A normálosztó tulajdonság ekvivalens módon jellemezhető az alábbiak szerint.

Állítás: (1) $N \trianglelefteq G \iff$ (2) $g^{-1}Ng = N\ \forall g \in G \iff$ (3) $g^{-1}ng \in N\ \forall g \in G,\ \forall n \in N$.

Biz: (1)$\Rightarrow$ (2): $Ng = gN \Rightarrow g^{-1}Ng = N$. (2)$\Rightarrow$ (3): $g^{-1}Ng = N \Rightarrow g^{-1}ng \in N$.
(3)$\Rightarrow$ (1): $g^{-1}ng \in N\ \forall n \in N \Rightarrow ng \in gN\ \forall n \in N \Rightarrow Ng \subseteq gN$. De $|Ng| = |gN|$ miatt $Ng = gN$ tetszőleges $g \in G$-re. □

Megfigyelés: Ha $N \trianglelefteq G$, akkor $(Ng)(Nh) = N(gN)h = N(Ng)h = (NN)(gh) = N(gh)$ tetszőleges $g, h \in G$-re. □

A fenti megfigyeles szerint a mellékosztályokon a komplexusszorzás művelet: két mellékosztályhoz rendel egy harmadikat. E műveletnek az egységeleme az N mellékosztály, és inverz is létezik: Ng inverze Ng^{-1}, hisz $NgNg^{-1} = Ngg^{-1} = N$.

Def: Ha $N \trianglelefteq G$, akkor az N mellékosztályainak csoportját a komplexusszorzásra a G csoport N szerinti *faktorcsoport*jának nevezzük, és G/N-nel jelöljük.

A faktorcsoport rendje nyilván N indexe, azaz $|G : N|$. Ha G Abel, akkor bármely H részcsoportja normálosztó, és a H szerinti faktorcsoport is Abel. Ha G mindezen túl ciklikus is, akkor a faktorcsoport is ciklikus lesz, és G minden generátorelemének mellékosztálya generálja a faktorcsoportot.

A normálosztók szoros kapcsolatban állnak a csoportok közötti, művelettartó leképezésekkel.

Def: Ha G és H csoportok, akkor a $\varphi : G \to H$ leképezés *homomorfizmus*, ha művelettartó, azaz bármely $g, g' \in G$ elemekre $\varphi(gg') = \varphi(g)\varphi(g')$. (Értelemszerűen, az egyenlőség baloldalán álló szorzás a G, a jobboldali a H csoportművelete.)

Ha φ homomorfizmus, akkor
$\mathrm{Ker}(\varphi) := \{g \in G : \varphi(g) = e_H\}$ a φ *magja*, és $\mathrm{Im}(\varphi) := \{\varphi(g) : g \in G\}$ a φ *képe*.

Megfigyelés: Ha $\varphi : G \to H$ homomorfizmus, akkor (1) $\varphi(e_G) = e_H$, (2) $\varphi(g^{-1}) = \varphi(g)^{-1}$, (3) $\mathrm{Ker}(\varphi) \trianglelefteq G$ és (4) $\mathrm{Im}(\varphi) \leq H$.

Biz:
(1): $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G) \Rightarrow e_H = \varphi(e_G)^{-1}\varphi(e_G) = \varphi(e_G)^{-1}\varphi(e_G)\varphi(e_G) = \varphi(e_G)$.
(2): $e_H = \varphi(e_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1}) \Rightarrow \varphi(g)^{-1} = \varphi(g^{-1})$
(3): Ha $\varphi(g) = \varphi(h) = e_H$, akkor $\varphi(gh) = \varphi(g)\varphi(h) = e_H e_H = e_H$, ill. $\varphi(g^{-1}) = \varphi(g)^{-1} = e_H^{-1} = e_H$, azaz $\mathrm{Ker}(\varphi) \leq G$. A normálosztó-tulajdonsághoz csak annyi kell, hogy tetszőleges $n \in \mathrm{Ker}(\varphi)$ és $g \in G$ esetén $g^{-1}ng \in \mathrm{Ker}(\varphi)$. Lássuk: $\varphi(g^{-1}ng) = \varphi(g^{-1})\varphi(n)\varphi(g) = \varphi(g)^{-1}e_H\varphi(g) = e_H$, csakugyan.
(4) Láttuk, hogy $\varphi(g^{-1}) = \varphi(g)^{-1}$, ill. $\varphi(gh) = \varphi(g)\varphi(h)$, azaz $\mathrm{Im}(\varphi)$ zárt az inverzképzésre és a H csoportműveletére, azaz $\mathrm{Im}(\varphi) \leq H$. □

Tehát minden homomorfizmus magja normálosztó. Ennek az állításnak a fordítottja is igaz, azaz minden normálosztó egyben homomorfizmus magja is, nevezetesen a $N \trianglelefteq G$ normálosztó a $\varphi_N : G \to G/N$ *természetes homomorfizmus* magja, mely a $\varphi_N(g) := Ng$ leképezéssel van megadva. (φ_N csakugyan homomorfizmus, hiszen $\varphi_N(gh) = Ngh = NNgh = NgNh = \varphi_N(g)\varphi_N(h)$.)

Homomorfizmus tétel: Ha $\varphi : G \to H$ csoport-homomorfizmus, akkor $G/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$.

Biz: Azt kell csak meggondolni, hogy φ bár G elemeit viszi H-ba, de egyúttal az $N := \mathrm{Ker}(\varphi)$ normálosztó mellékosztályain is homomorfizmus, amihez csak azt kell látni, hogy φ minden mellékosztályon konstans. Legyen $a, b \in Ng$ a g mellékosztályának elemei, azaz $a = ng$, $b = mg$ valamely $n, m \in \mathrm{Ker}(\varphi)$-re. Mivel $\varphi(n) = \varphi(m) = e_H$, ezért $\varphi(a) = \varphi(ng) = \varphi(n)\varphi(g) = \varphi(g) = \varphi(m)\varphi(g) = \varphi(mg) = \varphi(b)$. Tehát definiálható a $\varphi'(Ng) := \varphi(g)$ egy művelettartó $\varphi' : G/N \to H$ leképezést (azaz homomorfizmust) definiál. Az izomorfia igazolásához csak annyi kell, hogy a leképezés bijektív. Legyen hát $\varphi'(Ng) = \varphi'(Ng')$. Ekkor $\varphi(g) = \varphi(g')$, és g' felírható $g' = (g'g^{-1})g = fg$ alakban. Innen $\varphi(g) = \varphi(g') = \varphi(fg) = \varphi(f)\varphi(g)$, ahonnan $\varphi(f) = e_H$, azaz $f \in \mathrm{Ker}(\varphi) = N$, vagyis $g' \in Ng$, azaz $Ng' = Ng$. □

10.6. A kvaterniócsoport

A Q kvaterniócsoport elemei $1, -1, i, -i, j, -j, k, -k$, a szorzásműveletet definiálják (az asszociativitáson túl) az $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $(-1)^2 = 1$, $(-1)x = -x = x(-1)$, $-(-x) = x$, ill. az $1x = x1 = x$ ($\forall x \in Q$) azonosságok. Pl. $ji = j(jk) = j^2k = (-1)k = -k$. (A csoport-tulajdonság igazolásához az asszociativitást valóban ellenőrizni kell (kicsit fáradságos), egységelem az 1, a -1 inverze önmaga, a többi elem inverze a saját ellentettje.

Mivel $ij \neq ji$, ezért Q nem Abel csoport, így nem is ciklikus. Nem izomorf Q az ugyancsak 8-adrendű D_4 diédercsoporttal sem, mert Q-ban 1 rendje 1, -1 rendje 2, a többi elemé pedig 4, míg D_4-ben id rendje 1, minden tengelyes tükrözés ($t, f \circ t, f^2 \circ t, f^3 \circ t$) és a középpontos tükrözés (f^2) rendje 2, míg a forgatások (f, f^3) rendje 4. A Q kvaterniócsoport tehát különbözik az eddig megismert összes csoporttól.

11. Gyűrűk, testek

Eddig egyműveletes struktúrákkal foglalkoztunk. Ha azonban a $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ vagy $\mathbb{C}$ számhalmazokról szeretnénk többet tudni, érdemes mindkét alapműveletet (az összeadást és szorzást) figyelembe venni. Ez (is) indokolja az olyan algebrai struktúrák vizsgálatát, ahol két kétváltozós művelet értelmezett.

Def: A $\langle R, \{+, \cdot\}\rangle$ algebrai struktúra *gyűrű*, ha $\langle R, +\rangle$ Abel csoport, $\langle R, \cdot\rangle$ félcsoport, továbbá teljesülnek a *disztributív azonosságok*: $a(b+c) = ab + ac$ ill. $(a+b)c = ac + ab$ $(\forall a, b, c \in R)$. Ha röviden csak R gyűrűt mondunk, akkor konvenció szerint R két művelete $+$ és $\cdot$ a fentiek szerint.
Az R gyűrű *kommutatív*, ha a szorzás kommutatív. Az R gyűrű összeadásának egységelemét *nullelemnek* nevezzük, és 0-val jelöljük. Az R gyűrűben az $a \in R$ elem inverzét az összeadásra $-a$ jelöli. Az R gyűrű *egységelemes*, ha a szorzásműveletnek van egysége, melyet (ha van) 1 jelöl.

Megfigyelés: Ha R gyűrű, és $a, b \in R$, akkor $0a = a0 = 0$ ill. $(-a)b = -ab = a(-b)$.

Biz: A disztributivitás miatt $0 = 0a + (-0a) = (0+0)a + (-0a) = 0a + 0a + (-0a) = 0a$. Innen $-ab = -ab + 0 = -ab + 0b = -ab + (a + (-a))b = -ab + ab + (-a)b = (-a)b$. Az $a0 = 0$ ill. $-ab = a(-b)$ azonosságok hasonlóan következnek a baldisztributivitásból □

Példa: (1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ gyűrűk. $\mathbb{N}$ nem gyűrű, mert nem csoport az összeadásra (nincs inverz).
(2) Egy tetszőleges $n \in N$ szám többszörösei ($n\mathbb{Z}$) is gyűrű.
(3) A mod m maradékosztályok szintén.
(4) Az $n \times n$-es (racionális, valós vagy komplex) mátrixok is gyűrűt alkotnak.
(5) Az egész együtthatós polinomok $\mathbb{Z}[x]$ halmaza detto.
(6) A Gauss egészek (az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$) ugyancsak gyűrű.
(7) Tetszőleges H halmazra $\langle \mathcal{P}(H), \{\triangledown, \cap\}\rangle$ a H halmaz *Boole gyűrű*je, ahol $\triangledown$ a szimmetrikus különbséget jelöli: $A \triangledown B := (A \setminus B) \cup (B \setminus A)$. Itt a nullelem az $\emptyset$, az egység pedig a H.

Def: Az R gyűrűben a $a \neq 0$ elem *nullosztó*, ha létezik olyan $0 \neq b \in R$, melyre $ab = 0$. Az R gyűrű *nullosztómentes*, ha R-ben nincs nullosztó. Az R gyűrű *integritási tartomány*, ha kommutatív és nullosztómentes.

Példa: (1) $n\mathbb{Z}$ kommutatív és nullosztómentes, ezért integritási tartomány.
(2) $\mathbb{Z}_n$ nem nullosztómentes, ha vannak olyan $a, b \in \mathbb{Z}_n$ számok, melyekre $a \neq 0 \neq b$ (azaz $a \not\equiv 0 \not\equiv b (\mathrm{mod}\ n)$) és $ab \equiv 0 (\mathrm{mod}\ n)$, azaz ha n összetett. Ha $n = p$ prím, akkor a prímtulajdonság miatt, ha $ab = 0$, azaz $ab \equiv 0(p)$, vagyis $p \mid ab$, akkor $p \mid a$ vagy $p \mid b$, így $a = 0$ vagy $b = 0$ (a $\mathbb{Z}_p$ gyűrűben(!)). Tehát $\mathbb{Z}_p$ nullosztómentes, így integritási tartomány.
(3) Az $\mathbb{R}^{n\times n}$ mátrixgyűrűben A nullosztó, ha létezik olyan B mátrix, melyre $AB = \mathbf{0}$. Ez pontosan akkor van, ha az $Ax = 0$ egyenletnek van nemtriviális megoldása, azaz, ha A szinguláris.
(4) A $\langle \mathcal{P}(H), \{\triangledown, \cap\}\rangle$ Boole gyűrűben H minden valódi részhalmaza nulloszó, mert $A \cap (H \setminus A) = \emptyset$.

Def: Az R gyűrű *részgyűrűje* az $\langle R, \{+, \cdot\}\rangle$ olyan részstruktúrája, mely gyűrű. (Csupán a műveletekre való zártságot és az ellentettek meglétét (tkp a kivonásra való zártságot) kell ellenőrizni.)

Megfigyelés: Ha $n \in \mathbb{Z}$, akkor $n\mathbb{Z}$ a $\mathbb{Z}$ részgyűrűje. A $\mathbb{Z}$ gyűrű minden részgyűrűje $n\mathbb{Z}$ alakú.

Biz: Láttuk korábban, hogy $n\mathbb{Z}$ gyűrű. Ha R a $\mathbb{Z}$ részgyűrűje, akkor legyen $n := \min\{x \in R : x > 0\}$. Ekkor $0, n, -n, 2n, -2n, \ldots \in R$, ezért $n\mathbb{Z}$ az R részgyűrűje. Ha $m \in R$, akkor $m = qn + r$, ahol $0 \leq r < n$ az r maradékra. Mivel $r = m - qm \in R$, ezért n választása miatt $r = 0$, azaz $m \in n\mathbb{Z}$, vagyis $R = n\mathbb{Z}$.□

Láttuk, hogy a gyűrűben tudunk kivonni, azaz egy elem ellentettjét hozzáadni $(a - b := a + (-b))$. Felettébb bosszantó, hogy osztani nem tudunk, azaz nem tudunk egy elem inverzével szorozni, hiszen a szorzás nem csoport- (csak félcsoprt-) művelet, így nincs a szorzásra nézve inverz. Nyugodjunk meg: a szokásos számkörökben $(\mathbb{R}, \mathbb{C})$ sem tudunk osztani, mert az osztás nem *algebrai értelemben vett* művelet, hisz nem tudunk bármely két számot elosztani. Általában sem várhatjuk, hogy a gyűrűben a szorzásra nézve minden elemnek legyen inverze, hisz ha a x a 0 inverze, akkor $1 = 0x = (0+0)x = 0x + 0x = 1 + 1$, ahonnan $0 = 1$ adódik. Innen $0 = 0a = 1a = a$, azaz a gyűrű triviális, csak a 0 elemből áll. Kiderül, hogy a szorzás invertálhatósága nem kell, hogy ennél jobban sérüljön.

Def: A T gyűrű *ferdetest*, ha $\langle T \setminus \{0\}, \cdot\rangle$ csoport. Ha a szorzás kommutatív, akkor T *test*.

Példa: (1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ testek.
(2) Ha p prím, akkor $\mathbb{Z}_p$ test, melynek a szokásos jelölése $\mathbb{F}_p$. (Láttuk, hogy $\mathbb{Z}_p$ gyűrű, és a kis Fermat tétel mutatja a reciprok kiszámítását.) Ha m nem prím, akkor (láttuk) van $\mathbb{Z}_m$-ben nullosztó, aminek nincs reciproka, tehát $\mathbb{Z}_m$ nem test.
(3) A *valós polinomok hányadosteste* a következő. $\mathbb{R}(x) := \{\frac{p}{q} : p, q \in \mathbb{R}[x], q \not\equiv 0\}$. A műveletek: $\frac{p}{q} + \frac{r}{s} := \frac{ps+qr}{qs}$, ill. $\frac{p}{q} \cdot \frac{r}{s} := \frac{pr}{qs}$. (A polinomok hányadosteste a legszűkebb, az $\mathbb{R}[x]$ gyűrűt tartalmazó test. Ugyanazzal a konstrukcióval kapjuk, mint racionális számtestet, mely a legszűkebb, az egészek gyűrűjét tartalmazó test.)
(4) Az $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ halmaz is test, hiszen $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 + 2b^2$ miatt létezik inverz. ($\sqrt{2}$ helyett állhatna $\sqrt{t}$ is $(0 < t \in \mathbb{Q}_+)$.
(5) A *kvaterniók ferdeteste* a következő: $\{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$. Az összeadást a természetes módon definiáljuk, a szorzásnál pedig használjuk a Q-bel szorzást. Tény, hogy a szorzásra van inverz, de nem egészen triviális.

Tétel: Minden véges integritási tartomány test.

Biz: Az integritási tartományban a szorzás kommutatív, így csak azt kell bizonyítani, hogy létezik a szorzásnak egységeleme, és minden nemnulla elemnek van reciproka, azaz a szorzásra vonatkozó inverze. Legyen R véges integritási tartomány, és legyen $0 \neq a \in R$. Ha $ab = ab'$, akkor $0 = ab + (-ab') = ab + a(-b') = a(b + (-b'))$, ezért a nullosztómentesség miatt $b + (-b') = 0$, azaz $b = b'$. Eszerint az $ar_1, ar_2, \ldots$ elemek mind különbözőek (ahol $R = \{r_1, r_2, \ldots\}$), így R végessége miatt a teljes R halmaz előáll: $R = \{ar : r \in R\}$. Van tehát olyan $e \in R$, melyre $ae = a$. Azt szeretnénk igazolni, hogy e a szorzás egységeleme, azaz $be = b$ minden $b \in R$ esetén. A szorzás kommutativitása miatt $ab = (ae)b = a(eb) = a(be)$, azaz $0 = a(be) + (-ab) = a(be) + a(-b) = a(be + (-b))$, amiből a nullosztómentesség miatt $be + (-b) = 0$, azaz $eb = be = b$ adódik. Tehát R valóban egységelemes.

Láttuk, hogy rögzített $0 \neq a \in R$ esetén R minden eleme előáll ar alakban (alkalmas $r \in R$-re). Ez persze $e \in R$-re is igaz, tehát létezik olyan $r \in R$, melyre $ar = e$, azaz bármely $0 \neq a$-nak létezik inverze, vagyis R csakugyan test. □

Köv.: $\mathbb{Z}_p$ test, hiszen láttuk, hogy kommutatív gyűrű, és azt is hogy nullosztómentes, tehát $\mathbb{Z}_p$ véges integritási tartomány.

Def: A T test *prímtest*, ha nincs valódi részteste.

Megfigyelés: $\mathbb{Q}$ és $\mathbb{F}_p$ (ha p prím) prímtest, és más prímtest nincs.

Biz: Láttuk, hogy testek, és hogy $0 \neq 1$. Legyen T prímtest. Világos, hogy $n := 1 + 1 + \ldots + 1$ [n-szer] benne van T-ben. Ha $n = 0$ valamely $n > 0$-ra, akkor a $T = \mathbb{Z}_n$ a minimális ilyen n-re. Mivel T test, ezért n prím. Ha $n \neq 0$ minden $n > 0$-ra, akkor $0, 1, -1, 2, -2, \ldots$ mind T-beliek és különbözőek, tehát $\mathbb{Q} \subseteq T$. A T test prímtulajdonsága miattt ekkor $\mathbb{Q} = T$. □

Tétel: Ha T véges test, akkor elemszáma prímhatvány.

Biz: A T test vagy prímtest (ekkor a tétel triviális), vagy van valódi részteste, és így van egy valódi részteste is, mely prímtest, mondjuk $\mathbb{F}_p$. A T tekinthető a $\mathbb{F}_p$ test felett vektortérnek, mely véges (mondjuk n) dimenziós, ha T véges. Ekkor T elemszáma p^n, ami tényleg prímhatvány. □

12. Algoritmusok hatékonysága

A gyakorlatban számos problémát számítógéppel, algoritmikus úton oldunk meg. Gyakran több út is kínálkozik a cél elérésére, és nyilván azt érdemes választani, ami az adott problémát a leghatékonyabban kezeli. Ilyenkor össze kell hasonlítanunk különböző algoritmusokat, de máskor is fontos lehet, hogy egy eljárás gyorsaságáról tudjunk valamit mondani. Egy algoritmust képzelhetünk úgy, hogy egy miáltalunk megadott bemenethez egy kimenetet állít elő. A bemenetet gondolhatjuk a „kérdésnek", amit az algoritmusnak felteszünk, a kimenet pedig a kérdésre a „válasz". Nyilván, minél „nehezebb" a kérdés, annál több időt érdemes hagyni a számítógépnek a válaszra, azaz, annál több lépést tehet az adott algoritmus. Hogyan kell hát a kérdés „nehézségét" mérni? Egy célszerűnek látszó módszer az input „hossza": tehát az, hogy hány bit a bemenet, vagyis milyen hosszan írtuk le a problémát az algoritmus nyelvén. Az algoritmus meghatároz tehát egy $f : \mathbb{N} \to \mathbb{N}$ függvényt, mely minden n-re meghatározza azt az $f(n)$-t, ami az algoritmus legnagyobb lépésszáma egy n hosszú bemenet esetén. (Itt feltételezzük, hogy az algoritmus minden bemeneten előbb-utóbb megáll.) Ha egy A ill. A' algoritmus f ill. f' lépésszámfüggvényeire $f \leq f'$ áll, akkor jogos az A algoritmust hatékonyabbnak tekinteni, mint az A' algoritmust. Mi van azonban akkor, ha bizonyos n-ekre $f(n) < f'(n)$, más n-ekre pedig $f(n) > f'(n)$? Nos, ekkor az érdekel minket, hogy az input méretének növekedtével milyen gyorsan nő az algoritmus lépésszáma. A motiváció e mögött az, hogy nagyméretű feladatokat szeretnénk megoldani, és míg rövid input esetén a nagyobb lépésszám kompenzálható jobb számítógéppel, a bemenet méretének növekedtével ez nem tehető meg. Konkrétabban: ha az A algoritmus lépésszáma n hosszú inputon $10^5 \cdot n$, a A' algoritmusé pedig 2^n, akkor $n \leq 21$ esetén az A' algoritmus hatékonyabb, $n \geq 22$-re pedig az A. Ha tehát mondjuk 10^{10} lépést tudunk megengedni az algoritmusnak, hogy belátható időn belül eredményt kapjunk, akkor az A algoritmus $n \leq 10^5$ méretű bemenetken működik, míg az A' algoritmus számára $n \leq \log_2 10^{10} \leq \log_2 (10^3)^{\frac{10}{3}} = \frac{10}{3} \log_2 10^3 < \frac{10}{3} \cdot 10 < 34$ áll, azaz már a 34 hosszú bemenettel sem képes megbirkózni a program. A fenti példában a lényeges különbség a két algoritmuk között az volt, hogy míg az első maximális lépésszáma az inputméret *polinomjával* volt becsülhető, addig a másik algoritmus futásideje *exponenciális* függvénye is lehetett a bemenet hosszának. Jobbnak tekintünk tehát egy $10^{10^{10}} \cdot n^{10^{10}}$ lépésszámú algoritmust, mint egy $(1 + 10^{-10^{10}})^{10^{-10^{10}} \cdot n}$ futásidejűt, még akkor is, ha a gyakorlatban az előbbi már $n = 2$ méretű bemenet esetén kivitelezhetetlen, míg az utóbbi akkor is működik, ha a bemenet mérete a hihetetlenül hatalmas számok világából való. Még egyszer tehát az 1984-be illő szabály:

A polinomiális algoritmus jó, az exponenciális algoritmus rossz.

(A rend kedvéért tegyük hozzá, hogy ez így nem igaz. Itt és most azonban polinomiális lépésszámú algoritmusok érdekesek a számunkra.)

Megvizsgálunk néhány, számokkal operáló algoritmust hatékonyság szempontjából. Az algoritmus bemenete tehát néhány (általában két) szám, melyekkel műveletet végzünk. Először is gondoljuk meg, mi egy szám hossza. Itt az ésszerű eljárás a számot a szokásos módon megadni, ha nem is épp 10-es, de 2-es vagy mondjuk 16-os számrendszerben. Ekkor n hossza $\log_2 n$ ill. $\log_{16} n$ lesz, amik (mivel konstans szorzóban különböznek) az algoritmus polinomiális voltát nem befolyásolják. (Sőt, a polinom fokát sem, csupán a főegyüttható változik.) Mi tehát számrendszeralapú megadásban gondolkodunk, ekkor egy n és m szám együttes mérete $\log n + \log m$ lesz. A kérdés tehát, hogy ennek a számnak milyen függvénye egy-egy művelet lépésszáma.

Összeadás: Az általános iskolában tanult, írásbeli összeadás remekül működik más számrendeszerekben is. A műveletigény minden helyiértéknél legfeljebb 2, hisz két számot adunk össze az adott helyiértéken, plusz még egy esetleges maradékot az előző helyiértékből. A lépésszámra felső korlát tehát a $2 \cdot \max(\log n, \log m) < 2 \cdot (\log n + \log m)$, ami lineáris, vagyis polinomiális. A kivonásra hasonló igaz.

Szorzás: A szokásos írásbeli szorzás működik, és megvalósítható $\log n$ db összeadással, ahol minden összeadandó az m egy egyjegyű számmal összeszorzott többszöröse. Egy egyjegyű számmal m-t $2 \log m$ lépésben össze lehet szorozni, ugyanis minden jegyet szorozni kell, és az esetleges maradékot a szorzathoz hozzáadni. Tehát az összlépésszám $2(\log n)(\log m) \leq (\log n + \log m)^2$, vagyis a szorzás polinomiális. Az írásbeli osztás is polinom időben elvégezhető, de szőrözni kell pindurit, mikor megbecsüljük a soron következő hányadost.

Hatványozás: a n^m szám hossza $m \log n$, ami nem polinomiális függvénye $(\log n + \log m)$-nek. Mivel az algoritmus egy lépésben legfeljebb egy (pontosabban: konstans számú) jegyét tudja kiírni az eredménynek, már az eredmény megadása is exponenciálisan sok időt igényel, vagyis általában nem lehet polinomiális algoritmussal hatványozni.

Hatványozás modulo m: Legyen $m = \sum_i a_i 2^i$, azaz $m = \underline{\ldots a_2 a_1 a_0}_2$ a kettes számrendszerbeli alak. Sorra kiszámoljuk az $n_0, n_1, n_2, \ldots$ számokat, ahol $n_0 \equiv n(m)$, $n_1 \equiv n^2(m), \ldots, n_i \equiv n^{2^i}(m)$. Az n_{i+1}-t az $n_{i+1} \equiv n_i^2(m)$ alapján egy szorzással és egy maradékos osztással kaphatjuk, ráadásul n_i mérete mindig legfeljebb $\log m$ lesz. Tehát egy n_i kiszámítása egy legfeljebb $\log m$ méretű szám négyzetre emelését és a legfeljebb $2 \log m$ méretű eredmény maradékos osztását igényli. Az szükséges n_i-k kiszámításához mindezt $\log m$-szer kell megtenni. Az n^m meghatározását pedig $n^m = \prod_{i=1}^{\infty} a_i n^{2^i} \equiv \prod_{i=1}^{\infty} a_i n_i(m)$ alapján további, legfeljebb $\log m$ db, legfeljebb $\log m$ méretű szám szorzásával és $\log m$ db, legfeljebb $2 \log m$ méretű szám maradékos osztásával kapjuk. A modulo m hatványozás tehát összességében is polinomiális eljárás.

Euklideszi algoritmus: Az euklideszi algoritmus egy lépésében adott $a_i \leq b_i$ esetén kell egy maradékos osztást végezni, és meghatározni azt a $0 \leq a_{i+1} < a_i$-t, melyre $b_i = q_i \cdot a_i + a_{i+1}$ áll. A lépések során az a_i és b_i mérete legfeljebb akkora, mint n és m mérete közül a nagyobbik, tehát az Euklideszi algoritmus minden lépése polinomiális időt igényel. A nagy észrevétel, hogy $a_{i+2} \leq \frac{a_i}{2}$, ezért a fentieket legfeljebb $\log n$-szer kell elvégezni, amitől az eljárás polinomiális marad.

Prímtesztelés: Egy adott $n \in \mathbb{N}$ számról kell eldöntenünk, hogy prím-e. A bemenet mérete $\log n$, ennek polinomja lehet a lépésszám. Nem polinomiális tehát sem az Erathosztenészi szita, mely lépészszáma n-ben lineáris (ami $\log n$-ben exponenciális), sem a naív módszer, mely szerint 1-től $\sqrt{n}$-ig ellenőrizzük az oszthatóságot ($\sqrt{n}$-ben lineáris számú osztással).

A prímtesztelés kemény dió. Létezik olyan determinisztikus algoritmus, mely egyúttal polinomiális is, de ilyet csak a legutóbbi időben találtak. Ha azonban véletlen választást is megengedünk, akkor már nem annyira nehéz hatékony eljárást találni. A véletlen módszernek viszont az a sajátja, hogy ha csekély valószínűséggel is, de tévedhet. Olyan módszert mutatunk a továbbiakban, mely csak egyirányban tévedhet, azaz egy prímet sosem mond összetettnek de egy összetett számot esetleg („csillagászatian" kis valószínűséggel) prímnek gondolhat. A teszt alapja az Euler-Fermat tétel. Eszerint, ha egy n szám prím, akkor $k^{n-1} \equiv 1(n)$ minden $(k, n) = 1$ esetén. Ha tehát $(k, n) = 1$ és $k^{n-1} \not\equiv 1(n)$, akkor bizonyosan tudjuk, hogy n összetett, jóllehet, n egyetlen osztóját sem ismerjük. Az ilyen k számot az n szám *árulójának* nevezzük, hisz segítségével megtudtuk hogy n nem prím. Egy másik lehetőség, hogy rájöjjünk, hogy n összetett, ha találunk egy olyan $0 < k < n$ számot, melyre $(k, n) \neq 1$. Ekkor az Euklideszi algoritmus az n egy valódi osztóját is megtalálja, ezért az ilyen k számok még több információt adnak n-ről. Az ilyen k számok az n *leleplezői*. Persze az is megtörténhet, hogy n összetett, de egy $0 < k < n$ számra $k^{n-1} \equiv 1(n)$ áll. Ekkor k az n *cinkosa*, hisz nem árulja el, hogy n összetett. Igaz viszont, hogy ha van áruló, akkor az $1, 2, \ldots, n-1$ számok között legalább annyi áruló van, mint cinkos (és akkor a leleplezőkről még nem is beszéltünk).

Állítás: Ha $1 \leq c_1 < c_2 < \ldots < c_l < n$ az n szám cinkosai, és a az n egy árulója, akkor $ac_1, ac_2, \ldots ac_l$

az n szám páronként (modulo n) különböző árulói.

Biz: Ha $ac_i \equiv ac_j(n)$, akkor $(a,n)=1$ miatt $c_i \equiv c_j(n)$, azaz $c_i = c_j$, tehát az $ac_1, ac_2, \ldots ac_l$ számok valóban különböző maradékosztályokból valóak. Mivel $c_i^{n-1} \equiv 1(n)$ és $a^{n-1} \not\equiv 1(n)$, ezért $(ac_i)^{n-1} = a^{n-1}c_i^{n-1} \equiv a^{n-1} \not\equiv 1(n)$, tehát a fenti számok csakugyan árulók. □

(Egyébként a fenti bizonyításnál kicsit több igaz: a modulo n redukált maradékrenszer a szorzásra csoport, és a cinkosok ennek részcsoportját alkotják. Ha van áruló, akkor a részcsoport indexe legalább 2, így a részcsoport mérete legfeljebb fele a csoporténak.) A prímtesztelésre egy lehetséges módszer tehát a következő. Véletlenül választunk egy $0 < k < n$ számot. Ha k árulója vagy leleplezője n-nek, akkor kész vagyunk, n összetett. Ha k cinkos, akkor n-ről azt valószínűsítjük, hogy prím. Ezen az elgondoláson alapszik a *Fermat-teszt*.

Fermat-teszt
Bemenet: $n \in \mathbb{N}$. Kimenet: döntés, hogy n prím-e
begin
Legyen $0 < k < n$ véletlen szám
if $(k,n) \neq 1$, **then STOP:** n nem prím. (sőt: egy osztót is találtunk)
else if $k^{n-1} \not\equiv 1$ **then STOP:** n nem prím.
else STOP: úgy tűnik, n prím
end if
end if
end

Persze a Fermat-teszt hibázhat, de az előző állítás szerint a hibája csak az lehet, hogy egy összetettet számot prímnek mond. Ráadásul, ha n-nek van árulója, akkor a hiba valószínűsége legfeljebb $\frac{1}{2}$. Ha tehát m-szer választunk (egymástól független) véletlen számokat, akkor a hiba valószínűsége $\frac{1}{2^m}$ lesz, ami már $m = 100$-ra is elhanyagolható a hardverhibából eredő tévedés valószínűségéhez képest. Jegyezzük meg, hogy a többször (mondjuk 100-szor) megismételt Fermat-teszt polinomiális számú, polinomiális időben elvégezhető lépést használ.

Van azonban a Fermat-tesztnek egy hibája. Csak akkor működik, ha *létezik* n-nek árulója. Vannak azonban olyan számok (az ú.n. *álprímek*, vagy más néven *Carmichael számok*), melyeknek csak cinkosai és leleplezői vannak (utóbbiak elenyésző számban). Az ismételt Fermat-teszt ezeket a számokat majdnem biztosan prímnek találja. Olyan módszert szeretnénk, amely a mégoly ritka álprímekre is teljesen megbízhatóan működik. A Fermat-teszt a fő lépésében azt ellenőrzi hogy vajon $n \mid k^{n-1} - 1$ teljesül-e. Ha ugyanis n prím, akkor ez minden $0 < k < n$-re teljesül. Ennél azonban több is igaz. Ha ugyanis $n - 1 = 2^t \cdot q$, ahol q páratlan, akkor

$$k^{n-1} - 1 = (k^q - 1) \cdot (k^q + 1)(k^{2q} + 1)(k^{4q} + 1) \cdots (k^{2^{t-1}q} + 1) \,, \tag{1}$$

és ha n prím, akkor (1) jobboldalának valamelyik tényezőjét is osztja. Hiába osztható tehát a baloldal n-nel: ha a jobboldal egyetlen tényezője sem n többszöröse, akkor n összetett, és k az n szám egy *Carmichel értelemben vett árulója*[12]. Igaz, hogy minden összetett szám redukált maradékrendszerének legalább $\frac{3}{4}$-edrésze Carmichael értelemben vett áruló. Ezért az (1) jobboldalán álló szorzat tényezőinek n-nel való oszthatóságát vizsgáló *Miller-Rabin teszt* egy összetett számról legalább $\frac{3}{4}$ valószínűséggel azonnal megállapítja, hogy nem prím.

Miller-Rabin teszt
Bemenet: $n \in \mathbb{N}$. Kimenet: döntés, hogy n prím-e
begin
Legyen $0 < k < n$ véletlen szám
if $(k,n) \neq 1$, **then STOP:** n nem prím. (sőt: egy osztót is találtunk)
else if $k^q \equiv 1$ **then STOP:** n valószínűleg prím.
else i:=0, **loop while** i<t
if $k^{2^t q} \equiv -1$ **then STOP:** n vszg prím
else i:=i+1; **end if**
end loop
end if
end if
STOP: n összetett.
end

---

[12] Figyeljük meg, hogy ha k cinkos, de Carmichael értelemben vett áruló, akkor az (1) jobboldalán álló tényezők valamelyike leleplező, így az Euklideszi algoritmussal megtalálható n egy osztója is.

A Miller-Rabin tesztet függetlenül választott véletlen számokkal 50-szer megismételve a hiba valószínűsége gyakorlatilag 0-ra csökken. A Miller-Rabin teszt hatékonyságáról érdemes megemlíteni, hogy sokkal jobb, mint ahogy azt az elméleti becslés mutatja: mindössze egyetlen olyan szám van 1 és $2,5 \cdot 10^{10}$ között, melyet összetett, és ez a $k = 2, 3, 5, 7$-tel való tesztek után nem derül ki.

13. Nyilvános kulcsú titkosírások

A nyilvános kulcsú titkosírás az egyirányú függvény létezésére épít. A pontos definíció helyett nagyjából azt lehet mondani, hogy *egyirányú függvénynek* nevezünk egy $f : X \to X$ függvényt, ha f bijekció, mely hatékonyan (azaz polinomiális időben, és a gyakorlatban is gyorsan) számítható, azonban a fordított irányú f^{-1} lekpépezés kiszámítása pusztán f ismeretében reménytelen. (Pl. ha megvan a telefonkönyv, akkor egy adott személyhez hamrar telefonszámot tudok rendelni, de egy telefonszámhoz az előfizető megtalálása már korántsem ilyen hatékony csupán a telefonkönyvben bogarászva). Elképzelhető, hogy f egyirányú függvény, és f^{-1} kiszámítására is létezik hatékony eljárás. Persze ennek megtalálása pusztán f ismeretében (az egyirányúság definíciója szerint) reménytelen. Utóbbi függvényeket nevezzük *kiskapus egyirányú függvényeknek*. Rossz hír, hogy bár a nyilvános kulcsú titkosírási rendszerek erre a feltételezésre építenek nem tudjuk, vajon léteznek-e kiskapus egyirányú függvények. Vannak azonban függvények, melyekről azt *sejtjük*, hogy ilyenek, de ezt bebizonyítani nem tudjuk. (Így aztán mindig van min dolgozniuk a rejtjelfejtő szakembereknek.)

Egy titkosírási rendszernél rögzítjük a Σ ABC-t: ennek a jeleivel írjuk le az üzeneteinket. A kódolandó M üzenetről (M, mint message) feltehető, hogy t betűből áll, azaz $M \in \Sigma^t$, hiszen a hosszabb üzenetet t hosszúságú blokkokra vághatjuk, és minden blokkot külön üzenetnek tekinthetünk. A lehetséges üzeneteket azonosíthatjuk egy 0 és $|\Sigma|^t - 1$ közötti egész számmal pl azáltal, hogy Σ elemeit a $0, 1, \ldots, |\Sigma| - 1$ számoknak, magát az üzenetet pedig egy $|\Sigma|$ alapú számrendszerben felírt számnak gondoljuk. A nyilvános kulcsú titkosírási rendszert egy kiskapus egyirányú $f : \{0, 1, 2, \ldots, n-1\} \to \{0, 1, 2, \ldots, n-1\}$ függvény írja le[13], melyet egy ú.n. *nyilvános kulcs* segítségével egyértelműen megadunk, és mindenki számára hozzáférhetővé teszünk. Feltételezzük továbbá, hogy a célszemély (nevezzük A-nak; ő az, akinek a titkosított üzenetet el akarjuk juttatni) képes f^{-1} hatékony számítására, mert rendelkezik az f^{-1}-t leíró *titkos kulccsal*. Ha tehát el szeretnénk juttatni A-nak egy M üzenetet, nincs más dolgunk, mint kiszámítani $M' = f(M)$-t, melyet a nyilvános kulcs ismeretében könnyen megtehetünk. Ezután M'-t[14] bátran elküldhetjük A-nak. Ebből A hatékonyan ki tudja számítani $f^{-1}(M') = f^{-1}(f(M)) = M$-t, vagyis el tudja olvasni a pontos üzenetet. Bárki más, aki útközben lehallgatja az M' kódolt üzenetet, nem tudja abból M-t kihámozni, hisz még f-t ismerve sem tudja $f^{-1}(M)$-t megtalálni[15].

A nyilvános kulcsú titkosírás alkalmas a *digitális aláírás* megvalósítására is, azaz segítségével bizonyítható, hogy egy adott üzenet kitől érkezett. Nevezetesen, ha minden szereplőnek van egy kiskapus egyirányú függvénye, pl. A-e f_A, míg B-é f_B, akkor ha B alá akarja írni az m üzenetét, akkor A-nak az $M' = f_A(f_B^{-1}(M))$-t küldi el, amit A vissza tud fejteni f_A^{-1} és f_B ismeretében, hiszen $f_B(f_A^{-1}(M')) = f_B(f_A^{-1}(f_A(f_B^{-1}(M)))) = f_B(f_B^{-1}(M)) = M$. Ráádásul A bárki más (pl. a bíróság) számára is bizonyítani tudja, hogy az üzenetben az áll, amit állít, és hogy az üzenet B-től ered, hisz ha megmondja M-t, és $M^* := f_A^{-1}(M') = f_A^{-1}(f_A(f_B^{-1}(M))) = f_B^{-1}(M)$-t, akkor abból bárki ellenőrizheti a nyilvános kulcs ismeretében, hogy $M = f_B(M^*)$, vagyis, hogy B valóban aláírta az M üzenetet.

Nézzük meg, hogyan lehet a fenti sémát megvalósítani, azaz hogyan lehet egy kiskapus egyirányú függvényt megadni. Legyen p és q két prímszám, és legyen $n := pq$, $m := \varphi(n) = (p-1)(q-1)$. Válasszunk egy $1 \le e \le n$ számot, melyre $(e, m) = 1$ teljesül (ilyen e-t könnyen találhatunk), és legyen $f(M) := M^e (\mathrm{mod}\ n)$. Ezáltal $f : \{0, 1, 2, \ldots, n-1\} \to \{0, 1, 2, \ldots, n-1\}$ leképezés egy kiskapus egyirányú függvény lesz. A nyilvános kulcs tehát n és e megadása, hiszen ennek segítségével bárki hatékonyan ki tudja f-t számítani.

Az inverzleképezés kiszámításához először megoldjuk d-re az $ed \equiv 1 (m)$ kongruenciát, amit $(e, m) = 1$ miatt egyértelműen (és hatékonyan) megtehetünk. Aki nem ismeri m-t, annak ez a feladat (úgy hisszük) reménytelen. Az inverzleképezés pedig $f^{-1}(X) := X^d (\mathrm{mod}\ n)$ lesz. Valóban:

$$f^{-1}(f(M)) \equiv f^{-1}(X^e) \equiv (X^e)^d = X^{ed} = X^{lm+1} = X^{lm} \cdot X = (X^m)^l \cdot X = 1^l \cdot X \equiv X (\mathrm{mod}\ n)\ ,$$

[13] Ahhoz, hogy minden lehetséges üzenet kódolható legyen, az szükséges, hogy $n \ge |\Sigma|^t$ álljon.

[14] helyesebben egy M'-nek megfelelő karaktersorozatot, azaz $\Sigma^{t'}$ egy elemét, ahol $t' \ge t$

[15] Nem árt azért picit óvatosnak lenni. Ha a lehallgató tudja, hogy az üzenet pl. egy harci cselekmény kezdőnapját jelzi, akkor a nyilvános kulcs ismeretében kiszámíthatja az f(hétfő), f(kedd), ..., f(vasárnap) értékeket, és ha ezek egyikét fogta el, akkor mindent tud. Szóval nem érdemes ilyen után üzenni. Szerencsére vannak technikák, melyekkel ez a fajta támadás kivédhető. (Pl. minden t-es blokk egy kellően nagyméretű végszelete véletlen jeleket tartalmaz.)

az Euler-Fermat tétel miatt. (Itt kell, hogy $(X, n) = 1$, de könnyen belátható, hogy ez $p \mid X$ és $q \mid X$ esetén is igaz.) Tehát n és d ismeretében az inverzleképezés is hatékonyan számítható. Ráadásul n és d hatékonyan megkapható p, q és e ismeretében.

Miért gondoljuk, hogy a fent leírt f függvény valóban kiskapus egyirányú függvény? Csupán az egyirányúság szorul indoklásra, a kiskaput láttuk. Több jel mutat arra, hogy ha e-t jól választjuk (ennek miként je nem fér bele a jelen jegyzet kereteibe; lényeg, hogy létezik általánosan elfogadott módszer, mely biztosítja, hogy e alkalmas legyen), akkor n és e ismeretéből d meghatározása hasonlóan nehéz, mint n prímtényezőkre bontása. Az általános hiedelem szerint pedig ez reménytelen, ha a p és q prímszámok kellően nagyok. (Jelenleg a legalább 200-jegyűekben hisznek). (Természetesen ezért van, hogy először a prímeket választjuk, és azokból adódik n.) Csak az van hátra, hogy miként találunk alkalmas p és q prímeket. Mivel van hatékony prímtesztünk, ezért véletlen számokat generálva próba-szerencse alapon keresünk. Kérdés, hogy találunk-e belátható időn belül prímet. A valasz igen: a számelmélet egyik fontos eredménye, hogy a prímek sűrűsége n közelében nagyon jó közelítéssel $\frac{1}{\ln n}$, azaz e^{100} környékén véletlen számokat választva kb. $\frac{1}{100}$ valószínűséggel prímet találunk. Vagyis 200 próbálkozás után gyakorlatilag biztosan akad prím a horogra.