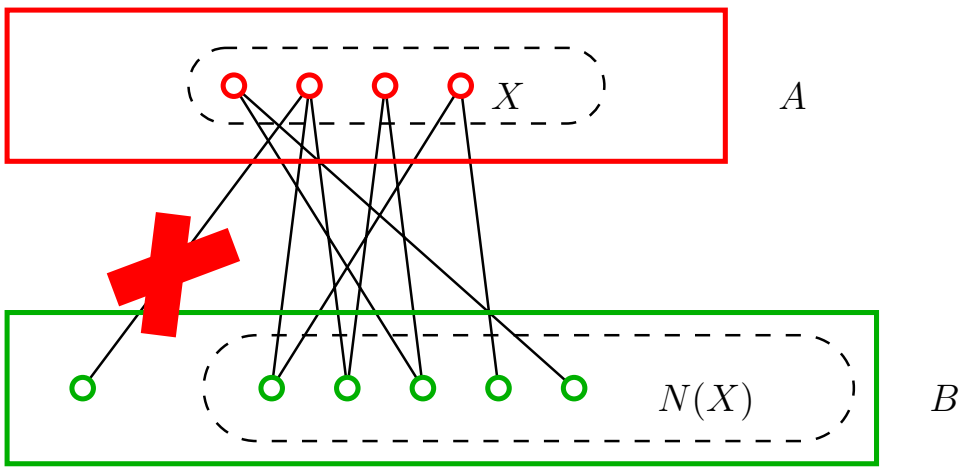
Bevezetés a számításelméletbe 2.

A BME I. éves mérnök-informatikus hallgatói számára

segédlet a 2008. tavaszi előadáshoz

Összeállította: Fleiner Tamás



Utolsó frissítés: 2011. május 23.

Tartalomjegyzék

Bevezetés

Ez a jegyzet nagyjából a BME-n, a 2007/2008-as tanév második félévében a mérnök-informatikus hallgatók számára előadott, VISZA 110 fedőnevű, „Bevezetés a számításelméletbe 2." c. előadás anyagát tartalmazza. A jegyzet elsődleges célja a vizsgára való felkészülés. Nem pótolja a rendelkezésre álló, könyvformátumú jegyzetet, amellyel számos tekintetben egyezik. Előnye mégis talán annyi, hogy szorosabban kapcsolódik az órán leadott anyaghoz, és így koncentráltabban tartalmazza a vizsgán számonkért tudást. A jegyzet valamennyire túl is mutat azonban az előadáson elhangzottakon, így olyan részeket is tartalmaz, amelyek ismeretét nem követeljük meg a vizsgán. Ha tehát valaki egészen véletlenül komolyabban érdeklődik egy-egy témakör iránt, 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 valódi szakirodalmat (is) érdemes tanulmányoznia.

Hogyan célszerű a jegyzetet használni, és egyáltalán: hogyan folyik a vizsga?

A jegyzetet igyekeztem úgy összeállítani, hogy abban minden szerepeljen, amit a vizsgán kérdezhetünk. Valószínűleg ez nem sikerült tökéletesen, de a szándék megvolt. A jegyzet a definíció-tétel-bizonyítás szentháromság alapján nyugszik: a definiált fogalmakat *dőlt betűs szedéssel* jeleztem, a tétel (állítás, megfigyelés, lemma) előtt **félkövéren** adom meg, miről is van szó, a bizonyítások végét pedig olyan kiskocka jelzi, mint amilyen pl. e sor végén is áll. □

Az is cél volt, hogy ne legyen túl száraz az anyag. A jegyzet ezért tartalmaz a tananyagot kiegészítő, ill. ahhoz kapcsolódó, érdekesnek ítélt információkat is. Az így közölt ismereteket a vizsgán tehát nem követeljük meg: az az általános irányelv, hogy az apró betűvel szedett részeket még a jeles osztályzatért sem kell tudni. Talán nem túl kockázatos azt kijelenteni, hogy a normál szedésű részek beható ismerete elegendő a jeles osztályzathoz. A spektrum másik végének teljesítésére már lényegesen több lehetőség kínálkozik. Elégtelent pl. úgy lehet szerezni, hogy a vizsgázó nem tudja pontosan kimondani valamelyik lényeges definíciót, tételt vagy állítást. Eredményes módszer az is, ha a definíciókat és tételeket szó szerint bemagolja a hallgató, de a vizsgán bemutatja, hogy nem érti, miről beszél. Más szóval: a legalább elégséges osztályzatnak feltétele a törzsanyaghoz tartozó fogalmak, állítások pontos ismerete, azaz, hogy a hallgató ezeket ki tudja mondani, képes legyen azokat alkalmazni és azokra szükség esetén példát mutatni. Az elégséges osztályzatnak nem feltétele, hogy minden ismertetett bizonyítást tökéletesen ismerjen a vizsgázó. Sőt: akár egyet sem kell tudni. Azonban aki ennek alapján próbál levizsgázni, az azt üzeni az őt vizsgáztatónak, hogy nagyon nem érdekli őt az anyag. Mint gyakorló vizsgáztató elmondhatom, hogy ez engem arra ösztönöz, hogy alaposan győződjek meg a definíciók és tételek kellő szintű ismeretéről, mert azt gondolom, hogy számos olyan állítást tartalmaz a tananyag, amit úgy a legkönnyebb megérteni, ha ismerjük a bizonyítást, vagy legalább annak vázlatát. Általánosságban elmondható, hogy sokkal fontosabb (értsd: elengedhetetlen), hogy egyetlen témakörben se lehessen zavarba hozni a vizsgázót, mint egy-egy bizonyítás részletes ismerete. Akinek „sajnos" nem jut ideje a ferdetest obskurus definícióját megtanulni, de hatosra tudja a Menger tételt, az éppúgy megbukik, mint az, aki semmit sem tud a prímszám definícióján kívül, és azt is csak alig.

A vizsga lebonyolítása úgy történik, hogy minden vizsgára jelentkező hallgatónak kisorsolunk egy tételt az itt is megtalálható tételsorból. Ezt követően legalább 45 perc felkészülési idő alatt a hallgató kidolgozhatja a tételét, célszerűen vázlatot ír. A számonkérés abból áll, hogy a kidolgozott vázlat alapján ki kell tudni mondani a vizsgatételben szereplő definíciókat és tételeket, illetve reprodukálni kell tudni a bizonyításokat. Ha nem megy magától, a vizsgáztató segít. Számítani kell arra is, hogy másik tétellel kapcsolatos fogalmakra, állításokra is rákérdez a vizsgáztató. A vizsgáztató személye a helyszínen dől

[1] Mint pl. ez is, itt.

el, az esetek többségében valamelyik előadó vagy gyakorlatvezető előtt kell számot adni a tudásról.

Hogyan is jött létre a jelen segédlet? A jegyzet írása 2004 tavaszán kezdődött, azóta hízik az anyag. Minden félév végén (legalábbis eddig) az előadáson elhangzottaknak megfelelően igazítok a tartalmon, és igyekeztem folyamatosan gyomlálni a jelentős számban felbukkanó hibákat is. (Volt, van, lesz belőlük bőven.) Ebben a harcban múlhatatlan érdemeket szereztek azok a hallgatók (és kollégák), akik jelezték, ha elírást vagy hibát találtak. Munkájukat ezúton is köszönöm. Remélem, hogy ennek nyomán a jegyzet használhatósága jelentősen javult, és számos későbbi hallgató felkészülését könnyíti meg. Természetesen mindehhez én is hozzáteszem a magamét: minden átdolgozáskor újabb elírásokat és tévedéseket illesztek az anyagba az egyensúly megőrzése érdekében.

Valószínűleg minden erőfeszítés ellenére valószínűleg számos hiba maradt a most közreadott jegyzetben is. Természetesen minden ilyen hiányosságért egyedül az enyém a felelősség. A jegyzettel, az abban található, akár helyesírási, nyelvhelyességi, akár módszertani, akár matematikai hibákkal kapcsolatos megjegyzéseket és a konstruktív hozzászólásokat köszönettel fogadom a `fleiner@cs.bme.hu` címen. Ünnepélyesen ígérem, hogy az érdemi kritika figyelembevételével igyekszem tovább javítani az anyagot. A jegyzet reményeim szerint karbantartott változata a `www.cs.bme.hu/~fleiner/jegyzet` weblapról tölthető le.

Pár szó végül a szerzői jogokról.

Minden olvasónak sikeres felkészülést és eredményes vizsgázást kívánok.

Budapest, 2008. május 21.

Fleiner Tamás

`Jegyzetevolúció-blog`

2008. 05. 16. 19.35: „Béta verzió!"

2008. 05. 21. 14.00: jegyzet 1.0. Átalakult a számelmélet rész utáni kongruenciákat tárgyaló szakasz. A pdf azt hiszem, fapados, ha vkinek ez gond, szóljon. Zsolnay Károly és Vandra Ákos vett észre hibákat, ezeket javítottam.

2008. 06.09. 16.00: jegyzet 1.1. Rádi Attila talált hibákat. Sajnos nem tudtam megírni pár kiegészítést, amit majd egyszer talán megteszek.

2008. 06.12. 15.40: jegyzet 1.2. Hidasi Péter és Virág Dániel találtak hibákat.

2009. 06. 22. 19.00: jegyzet 1.3 Joó Ádám, Szárnyas Gábor és Vőneki Balázs segítettek.

2010. 05. 10. 12.20: jegyzet 1.4 Wiener Gábor segített.

2011. 05. 23. 18.00: jegyzet 1.5 Bui Duy Hai vett észre több pontatlanságot.

Bevezetés a Számításelméletbe II. vizsgatételek
(2007/2008. második félév)

1. Euler-körök és -utak, ezek létezésének szükséges és elégséges feltétele. Hamilton-körök és -utak. Szükséges feltétel Hamilton-kör/út létezésére. Elégséges feltételek: Dirac és Ore tétele.

2. Gráfok színezése, kromatikus szám. A kromatikus szám becslései a klikkszám, a maximális fokszám és a független pontok maximális száma segítségével. Brooks tétele (biz. nélkül). Mycielski konstrukciója.

3. Síkbarajzolható gráfok kromatikus száma. Perfekt gráfok, Lovász gyenge perfekt gráf tétele (biz. nélkül), erős perfekt gráf tétel (biz. nélkül), intervallumgráfok perfektsége. Élkromatikus szám, viszonya a maximális fokszámhoz, Vizing-tétel (biz. nélkül).

4. Hálózat, hálózati folyam és (s,t)-vágás fogalma, folyam nagysága, (s,t)-vágás kapacitása. Ford-Fulkerson tétel, Edmonds-Karp tétel (biz. nélkül), egészértékűségi lemma. A folyamprobléma általánosításai.

5. Menger tételei. Többszörös összefüggőség és élösszefüggőség. Dirac tétele (biz. nélkül).

6. Páros gráf fogalma, karakterizációja. Párosítások páros gráfban, a javítóutas módszer. Kőnig, Hall és Frobenius tételei.

7. Párosítások tetszőleges gráfban, Tutte tétele (csak a könnyű irány bizonyításával). Gallai tételei. Gráfok és mátrixok: szomszédsági mátrix és hatványainak jelentése, illeszkedési mátrix és rangja.

8. Oszthatóság, felbonthatatlanok, a számelmélet alaptétele. Legnagyobb közös osztó, legkisebb közös többszörös, osztók száma. Euklideszi algoritmus. Nevezetes tételek prímszámokról: prímek száma, hézag a szomszédos prímek között, Csebisev-tétel (biz. nélkül), Dirichlet tétele (biz. nélkül).

9. Kongruencia fogalma, alapműveletek kongruenciákkal. Lineáris kongruenciák megoldása Euklideszi algoritmussal, a megoldhatóság feltétele, megoldások száma.

10. Teljes és redukált maradékrendszer fogalma, φ-függvény, kiszámítása. Euler-Fermat tétel, kis Fermat-tétel.

11. Művelet fogalma, félcsoport, csoport, Abel-csoport. Csoportok számokon, mátrixokon, diédercsoport. Példák véges és végtelen, kommutatív és nem kommutatív csoportra, mind a négy lehetséges variációban.

12. Elem rendje, részcsoport, generált részcsoport, ciklikus csoport. Mellékosztályok, Lagrange tétele, következménye az elemek rendjére vonatkozóan. A szimmetrikus csoport. Csoportok izomorfiája, Cayley tétele.

13. Gyűrű és test fogalma, véges és végtelen példák. Számelmélet és algoritmusok: összeadás, szorzás, maradékos osztás, hatványozás lépésszáma. Modulo m hatványozás polinomiális időben.

14. Prímtesztelés, Carmichael számok. Nyilvános kulcsú titkosírás és digitális aláírás fogalma, megvalósításuk RSA-kódolás segítségével.

1. fejezet

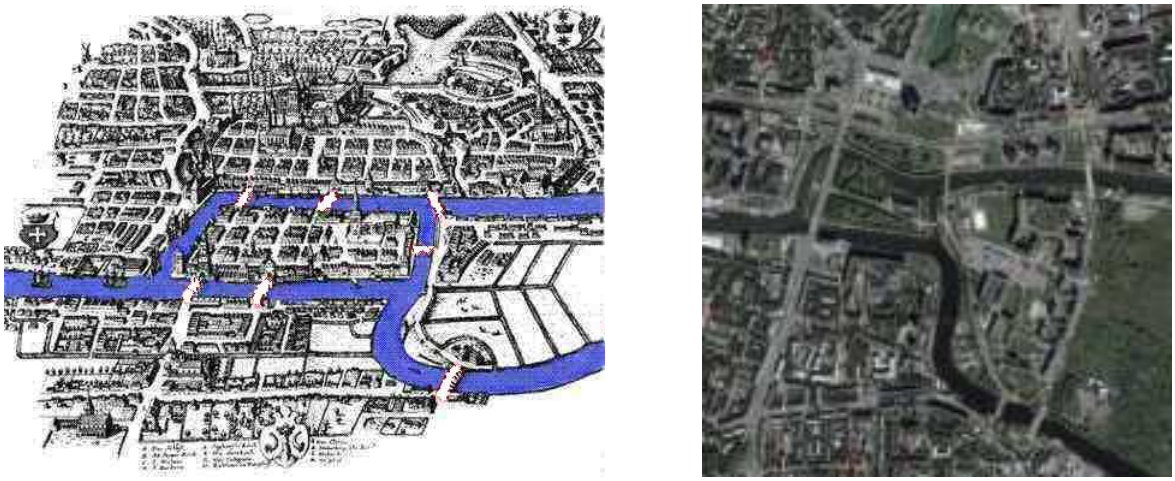
Gráfelmélet

1.1 Euler és Hamilton bejárások

Def.: A $G = (V, E)$ gráf *Euler-sétája (Euler-körsétája)* a G gráf egy olyan (kör)sétája, amely G minden élét pontosan egyszer tartalmazza.

Voltaképpen a G gráf éleinek olyan bejárásáról van szó, melyben minden élt pontosan egyszer érintünk. Ez a rejtvényújságokban szokásos, „rajzoljuk le egy vonallal, a ceruza felemelése nélkül" típusú fejtörő absztrakt változata: ha a lerajzolandó ábrát egy (síkbarajzolt) gráf diagramjának 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-sétája.

A gráfelmélet születését a „Königsbergi hidak problémájának" megoldásához szokás kötni. 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.



1.1. 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.[1]

[1] Jegyezzük meg, hogy Königsberg mai neve Kalinyingrád, és a Kalinyingrádi Orosz Exklávé székhelye. Az exklávé annyit tesz, mint Oroszország olyan összefüggő komponense, amely 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 egyetlen fagymentes balti tengeri 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 jelenlegi hidak közül már

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

Biz.: A séta éleit az azokon való áthaladás szerint irányítva minden v csúcs befoka (azaz a v-be befutó élek száma) azonos lesz v kifokával (azaz a v-ből kiinduló élek számával), kivéve esetleg az első és utolsó csúcsot. A v csúcs fokszáma pedig a kifoka és befoka összege, tehát ha ezek egyenlőek, akkor $d(v)$ feltétlenül páros. □

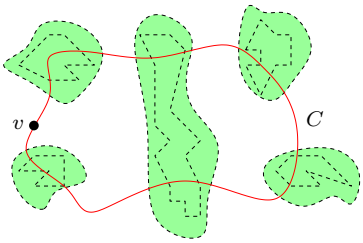
Az iménti szükséges feltételnek az értelmes megfordítása is igaz.

Tétel: [2] Ha a $G = (V, E)$ gráf véges és összefüggő, akkor

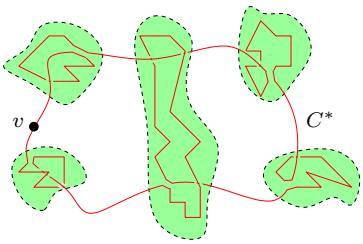
1. G-nek pontosan akkor van Euler-körsétája, ha G minden csúcsa páros fokú, ill.
2. G-nek pontosan akkor van Euler-sétája, ha G-nek 0 vagy 2 páratlan fokú csúcsa van.[3]

Biz.: 1.: A szükségesség a fenti megfigyelésből következik. Az elégségességet G élszáma szerinti indukcióval bizonyítjuk. 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.

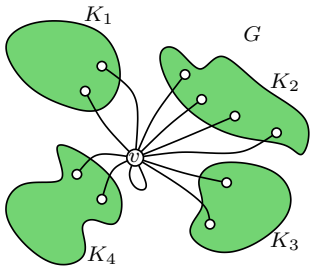
G-ben létezik egy C kör, mert minden fokszám legalább kettő: ha elindulunk G egy tetszőleges csúcsából, és mindig csatlakozó éleken lépünk tovább, akkor egyszer egy korábban érintett v csúcsba kell jutnunk, hisz elsőfokú pont híján sosem akadhatunk el. A v csúcs két érintése között pedig éppen egy kört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



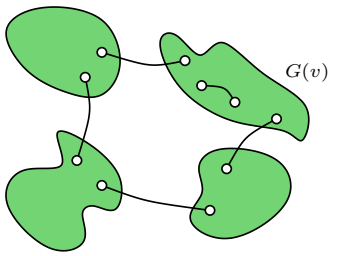
Tekintsük a $G' = G - C$ gráfot, mely C éleinek törlésével keletkezik G-ből. G' minden egyes komponense véges, öf, m-nél kevesebb élt tartalmaz, és minden fokszáma páros, ezért az indukciós feltevés miatt minden komponensnek van Euler-körsétája. A G gráf C^* Euler-körsétáját úgy kapjuk, hogy a C kör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



Megadunk a tétel első részében az elégségességre egy másik lehetséges bizonyítást. Ez G csúcsainak számára vonatkozó teljes indukcióval történik. Ha G-nek egyetlen csúcsa van, akkor G-nek csak hurokélei lehetnek; ezek pedig tetszőleges sorrendben felsorolva egy Euler-körsétát alkotnak. Tegyük fel tehát, hogy az $n-1$ csúcsú gráfokra már tudjuk az állítást, és legyen G-nek n csúcsa, ezek egyike legyen v. Legyenek $K_1, K_2, \dots K_s$ a $G - v$ gráf komponensei. Állítjuk, hogy v-ből legalább két él vezet mindegyik K_i-be. Mivel G öf, ezért v és K_i közt van él. Ha tekintjük a v és K_i által feszített $G[K_i + v]$ részgráfot, akkor ez minden K_i-beli végponttal rendelkező élt tartalmaz, ezért $G[K_i + v]$ minden K_i-beli pontjának fokszáma páros. A $G[K_i + v]$ gráf fokszámösszege azonban csak úgy lehet páros, ha v foka is páros, ami eszerint legalább 2.



Azt kaptuk tehát, hogy v-ből $G - v$ minden komponensébe legalább két él vezet. Most végezzük el a következő átalakításokat. Hagyjuk el a v-re illeszkedő hurokéleket. Rendezzük párokba a v-ből induló (nem hurok)éleket, és ha vu, vw egy ilyen élpár, akkor helyettesítsünk azokat egy uw éllel. Arra kell azonban ügyelnünk, hogy az élek párosítását úgy végezzük el, hogy minden K_i-re legyen olyan vu, vw élpár, hogy u a K_i, w pedig a K_{i+1} pontja (ahol $K_{s+1} = K_1$). Hagyjuk el ezután a v csúcsot. A keletkező $G(v)$ gráf öf lesz (hisz a K_i komponenseken „körbe" lehet menni. Ráadásul $G(v)$-nek $n-1$ csúcsa van, és $G(v)$-ben minden csúcs foka megegyezik az adott csúcs G-beli fokával, tehát páros. Az indukciós feltevés szerint tehát létezik $G(v)$-nek Euler körsétája. Ebből úgy kapjuk meg G egy Euler körsétáját, hogy minden alkalommal, amikor $G(v)$ egy újonnan bevezetett élén haladunk végig, olyankor e helyett a megfelelő két élt járjuk be, és áthaladunk v-n, majd a körséta végére biggyesztjük a v-beli hurokélek bejárását. Ez pedig azt jelenti, hogy G-nek létezik Euler körsétája, azaz igazoltuk az indukciós lépést.



2.: Ha G minden csúcsának foka ps, akkor 1. miatt létezik Euler-körséta, ami egyúttal Euler-séta is. Egyébként húzzunk be G ptn fokú csúcsai között egy új e^* élt. 1. miatt a keletkező G' gráfnak létezik

csak kettő emlékeztet a korabeliekre. Egy hidat a németek 1935-ben építették újjá, míg kettőt a Brit hadsereg bombázott le a történelmi városközpont megsemmisítésekor, 1944 augusztusában. Később, a szovjet időkben további két hidat váltottak ki újakkal. (Ld. az ábrát)

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

[3] Jó, jó, de mi van akkor, ha G-nek pontosan egy páratlan fokú pontja van? Az elsőnek tanult gráfos tétel segít...

Euler-körsétája, feltehetjük, hogy e^* a kör utolsó éle. Az e^* él Euler-körsétából való törlésekor éppen G egy Euler-sétáját kapjuk. □

A fenti tétel bár irányítatlan gráfokról szólt, irányított gráfokra is hasonló eredmény mondható ki. Az Euler-séta ill. körséta irányított változata a definíció értelemszerű módosításával kapható meg, és a páros fokszámokra vonatkozó állítás az alábbiak szerint módosul.

Állítás: Ha a véges, irányított G gráfnak létezik Euler-körsétája, akkor G minden csúcsának ugyanannyi a befoka mint a kifoka, azaz tetszőleges v csúcsra igaz, hogy a v-be befutó élek száma megegyezik a v-ből kiinduló élek számával. Ha Euler-sétája van G-nek, akkor lehet két kivételes csúcs: az egyikben a befok eggyel több a kifoknál, a másiknál a kifok nagyobb a befoknál eggyel.

A bizonyítás a fenti bizonyítás értelemszerű módosítása. A fenti tétel alábbi megfordítása teljesül.

Tétel: Ha a $G = (V, E)$ irányított gráf véges és irányítatlan értelemben összefüggő, akkor

1. G-nek pontosan akkor van Euler-körsétája, ha G minden csúcsába ugyanannyi él fut be, mint ahány onnan kilép, ill.

2. G-nek pontosan akkor van Euler-sétája, ha G-be behúzható legfeljebb egy irányított él úgy, hogy a kapott gráf rendelkezzen az 1. pontban megfogalmazott tulajdonsággal.

Bármelyik fent közölt bizonyítás értelemszerű módosítása igazolja a fenti tételt. Ez az irányított változat a Menger tételnél lesz hasznos a továbbiakban. Jegyezzük meg azt is, hogy sem az irányítatlan, sem pedig az irányított változatnál nem kellett feltenni a szóbanforgó gráf egyszerűségét: az elmondott bizonyítások működnek párhuzamos és hurokélek megléte esetén is. (A második bizonyítás lényegesen támaszkodott is erre.)

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

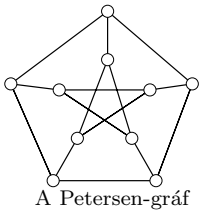
Megjegyzés: Mivel egy körben (útban) szereplő minden csúcs különböző, ezért a Hamilton-kör (Hamilton-út) a G gráf olyan bejárása, mely G minden csúcsát *pontosan* egyszer érinti.

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 páronként 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.

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. (Ha $a = 0$ vagy $b = 0$, akkor az adott körön egy komponens keletkezik, de ennek a komponensnek a „másik" körből is lesz pontja.)


A Petersen-gráf

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 $d(u) + d(v) \geq n$ (azaz összekötetlen csúcsok fokszámösszege legalább 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.

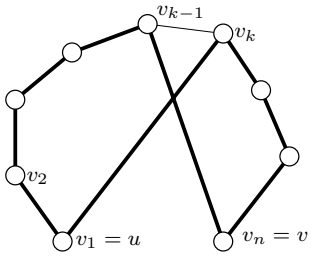
Állítás: Ha egy gráfra teljesül az Ore feltétel, akkor teljesül rá a Pósa is. Ezért az Ore tétel következik a Pósa tételből.

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 egy $d_1 \leq d_2 \leq \ldots \leq d_n$ sorozatra nem teljesül az előző feltétel, akkor van olyan G' gráf, aminek nincs Hamilton-köre, és fokszámainak $d'_1 \leq d'_2 \leq \ldots \leq d'_n$ sorozatára $d_i \leq d'_i \ \forall i = 1, 2, \ldots, n$ áll fenn.

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: Legyen 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. Feltehető, hogy $k < l$. (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 tételnél. 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.

1.2 Gráfok színezései

Def.: A G gráf k *színnel színezhető*, ha G minden csúcsa kiszínezhető k adott szín valamelyikére úgy, hogy G bármely élének két végpontja különböző színű legyen. A G gráf *kromatikus száma* $\chi(G) = k$, ha G kiszínezhető k színnel, de $k - 1$ színnel még nem.

Amikor egy gráf *kiszínezéséről* beszélünk (hacsak nem jelezzük az ellenkezőjét), mindig a csúcsoknak a fenti szabály szerinti színezésére gondolunk. Egy konkrét színezés esetén az azonos színűre festett csúcsok halmazát (amely halmaz tehát nem feszíthet élt) *színosztálynak* nevezzük. Jegyezzük meg, hogy a színosztály mindig a színezéstől függ, és általában nem egyértelmű, hogy egy G gráfot hogyan is kell $\chi(G)$ színnel kiszínezni.

Megjegyzés: 1. Ha G k-színezhető, akkor G-ben nincs hurokél, hisz egy hurokél végpontját nem lehet a fenti szabály szerint megszínezni.
2. A G gráf k-színezése tkp. egy olyan $c : V(G) \to \{1, 2, \ldots, k\}$ leképezés, melyre $c(u) = c(v) \Rightarrow uv \notin E(G)$ teljesül. (Ez a formális definíció.)
3. A G gráf egy (adott színezéshez tartozó) színosztályának csúcsai között nem fut él. A lehetséges színosztályokról szól a következő definíció.

Def.: A G gráf csúcsainak U részhalmaza *független*, ha G-nek nincs olyan éle, melynek mindkét végpontja U-beli. A G gráf *független csúcsainak maximális száma* $\alpha(G) = l$, ha létezik G-nek l pontú független ponthalmaza, de $l + 1$ páronként összekötetlen csúcs már nincs G-ben.

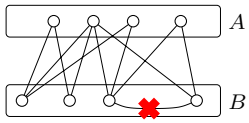
A kromatikus számot ezek szerint úgy is definiálhatjuk, hogy $\chi(G)$ a legkisebb olyan k egész, melyre G csúcshalmaza lefedhető k független ponthalmazzal.

Mik azok a gráfok amiket egy színnel kiszínezhetünk, azaz mit jelent, hogy $\chi(G) = 1$? Világos, hogy amint G-nek van éle, a két végpontjára két különböző színt kell használni, illetve, ha G egy ú.n. *üresgráf*, aminek minden csúcsa izolált, akkor egy szín elegendő. Tehát az 1-színezhető gráfok éppen az üresgráfok (azaz a teljes gráfok komplementerei). Ennél izgalmasabb osztályt alkotnak azok a gráfok, amikhez két szín elegendő.

Def.: A G gráf páros gráf, ha G két színnel kiszínezhető, azaz, ha $\chi(G) \leq 2$.

Megjegyzés: A fenti definíció azzal ekvivalens, hogy a G gráf pontosan akkor páros, ha G csúcsai két diszjunkt halmazba oszthatók úgy, hogy G minden éle a két halmaz között fut, azaz mindkét halmazban van egy-egy csúcsa. (Ez egyébként a páros gráf szokásos definíciója.) Minden páros gráfnak van tehát két színosztálya, amik között az élei futnak. Azonban ez a két színosztály nem feltétlenül egyértelmű:

pl az n pontból álló üres gráf csúcsainak tetszőleges két osztályra bontása teljesíti a feltételt. (Könnyen látható, hogy a két színnel való színezés pontosan akkor egyértelmű, ha a páros gráf öf.)



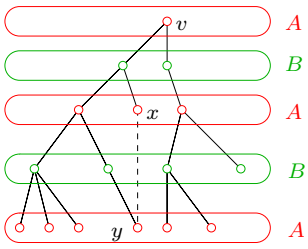
Ha hangsúlyozni akarjuk, hogy a szóbanforgó $G = (V, E)$ gráf *páros*, és egyúttal az A és B színosztályokat is meg szerenénk adni, akkor használhatjuk a $G = (A, B; E)$ jelölést.

Megfigyelés: 1. Minden páros hosszú kör páros gráf, t.i. felváltva ki lehet színezni a csúcsait két színnel.
2. Páratlan körre ezt nem tehetjük meg, mert mikor körbeérünk, két azonos színű pont szomszédos lesz. A páratlan kör tehát nem páros gráf.
3. Ha egy gráf páros, akkor minden részgráfja is páros.
4. 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 megfigyelésből közvetlenül adódik.



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. (Pl. $v \in A$.) 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 $xy \dots v \dots x$ 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, ami ellentmondás. □

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 $\omega(G) \le \chi(G) \le \Delta(G) + 1$ valamint $\chi(G) \ge \frac{n}{\alpha(G)}$ teljesül, ahol n a G csúcsainak számát jelenti.

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

Másrészt az ún. mohó színezés mutatja, hogy bármely G gráf $(\Delta(G)+1)$-színezhető. Színezzük ki G pontjait $v_1, v_2, \dots v_n$ 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.

A tétel második része azért igaz, mert ha G-t kiszínezzük $\chi(G)$ színnel akkor minden egyes színosztály legfeljebb $\alpha(G)$ méretű, hisz független pontokból áll. Ezek szerint G csúcsait $\chi(G)$ darab, legfeljebb $\alpha(G)$ méretű halmaz uniójára bontottuk, ahonnan $n \le \chi(G) \cdot \alpha(G)$, és innen az állítás közvetlenül adódik. □

Megjegyzés: A fenti állításban egyik egyenlőtlenséget sem lehet *általában* megjavítani: az első alsó becslés pl. az ún. perfekt gráfokra éles, és a második alsó becslésre is könnyű azt egyenlőséggel teljesítő gráfot konstruálni. 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 $\chi(G) \le \Delta(G)$. □

A Brooks tétel egy gyengített változatát igazoljuk.

Tétel: Ha a G véges gráf összefüggő és G nem reguláris, akkor $\chi(G) \le \Delta(G)$.

Biz.: A tétel azzal ekvivalens, hogy G kiszínezhető $\Delta(G)$ színnel. Ezt a mohó színezéssel fogjuk megmutatni. Láttuk, hogy a mohó színezéskor legfeljebb eggyel több színt használunk fel, mint ahány korábban kiszínezett szomszédja lehet G egy csúcsának. A $\Delta(G)$ színnel való színezés lehetősége következik tehát abból, ha G csúcsainak sikerül olyan $v_1, v_2, \dots, v_n$ sorrendjét megadnunk, amire az teljesül, hogy minden v_i-nek legfeljebb $\Delta(G) - 1$ kisebb indexű szomszédja van. A $v_1, v_2, \dots, v_n$ sorrend viszont

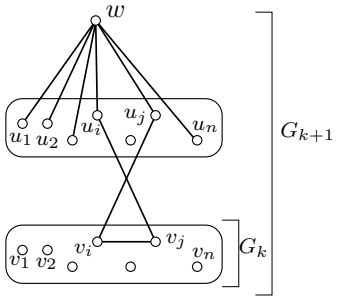
automatikusan ilyen lesz, ha az teljesül rá, hogy v_n kivételével minden v_i-nek van i-nél nagyobb indexű szomszédja, továbbá, hogy v_n fokszáma $\Delta(G)$-nél kisebb.

Mivel G nem reguláris, létezik $\Delta(G)$-nél kisebb fokszámú csúcsa, legyen ez v_n. Tekintsük G egy F feszítőfáját (ami G öf tulajdonsága miatt létezik), legyen ennek v_1 egy v_n-től különböző levele. Ilyen van, hisz minden (legalább kétpontú) fának van legalább két levele. Legyen v_2 az $F - v_1$ fa egy v_n-től különböző levele, és így tovább, azaz v_i az $F - \{v_1, v_2, \ldots, v_{i-1}\}$ fa egy v_n-től különböző levele. Ez a Prüfer kódoláshoz hasonló levéltörlési eljárás a G gráf csúcsainak olyan $v_1, v_2, \ldots, v_n$ sorrendjét határozza meg, amire v_n nem maximális fokszámú, és minden más v_i-nek van a sorrendben őt követő szomszédja is. Nekünk pedig pontosan erre volt szükségünk a tétel bizonyításához. □.

Az alábbi tétel pedig 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 valamely k-ra 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. A háromszög harmadik pontja nem lehet w, hisz az nem szomszédos egyik v_i-vel, és nem lehet G_k-nak sem pontja, hisz G_k az indukciós feltevés szerint nem tartalmaz háromszöget. Ha tehát a háromszög a harmadik pontja mondjuk u_l, akkor G_{k+1} definíciója v_i, v_j, v_l a G_k-ban háromszöget alkotnak, ami ismét csak 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 a G_{k+1} gráf $k+1$ színnel színezhető, azaz, 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 a megfelelő u_i csúcs színére. Ezáltal a $\{v_1, v_2, \ldots, v_n\}$ pontok mindegyike w-étől különböző színt kap. Tehát G_k pontjai $(k-1)$-féle színt kaptak. Az indukciós feltevés szerint $\chi(G_k) = k > k-1$, ezért G_k nem színezhető jól $k-1$ színnel, vagyis 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: mint látni fogjuk, annak a felismerése, hogy egy adott G gráf 3-színezhető-e (azaz G csúcsai előállnak-e 3 független ponthalmaz uniójaként), bizonyíthatóan nehéz. Érdekes viszont, 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[4]. Más szóval, egy síkbarajzolt gráf tartományait kell színeznünk, ami ekvivalens az adott gráf duálisának színezésével.

A 4-szín tételt először Francis Guthrie sejtette meg 1852-ben: megfigyelte, hogy Anglia megyéi úgy 4-színezhetőek, hogy szomszédos megyék különböző színt kapnak. Többszörös áttétellel értesült erről Cayley, aki nem talált bizonyítást, ezért 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 hibák egyikét sem sikerült azóta sem kijavítani. Sokak hosszú, eredménytelen próbálkozásai után Appel és Haken 1976-ban jelentették be, hogy igazolták 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

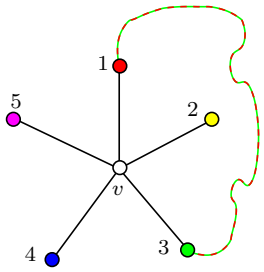
[4]Ez sem egészen igaz, ugyanis a politikai térképek nem szükségképpen 4-színezhetőek, hisz pl. Kalinyingrádot is az Oroszországhoz használt színnel kell festeni. Ha ezt jól megértettük, akkor nem meglepő az az állítás sem, hogy tetszőleges k-hoz létezik olyan politikai térkép, ami nem színezhető ki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

számítógép programja valóban azt végzi el, amit arról feltételezünk. A történet következő allomásához 1996-ban érkezett, amikoris Robertson, Sanders, Seymour és Thomas talált egy, az Appel-Haken-félénél jóval egyszerűbb bizonyítást, mely arra vezet, hogy 633 kis gráf ú.n. redukálhatóságát kell ellenőrizni. Természetesen Robertsonék is számítógéppel végeztették ezt el, ezért továbbra sem lehetünk abszolút bizonyosak afelől, hogy a bizonyítás korrekt. Sajnos ezen ma sem tud senki segíteni. Történt azért még valami, ami említést érdemel. Ha nincs ember, aki ellenőrizhetné a bizonyítást, miért ne tehetné meg azt a gép? Léteznek ugyanis mechanikus bizonyításellenőrző programok, ezek egyike az ú.n. coq. 2004-ben Georges Gonthier átírta Robertson és társai bizonyítását a bizonyításellenőrző által értelmezhető formális nyelvre, és ellenőriztette azt. A munka egyáltalán nem volt triviális, és bár a teszt sikeres volt (úgyhogy mostanra aztán tovább csökkentek a kételyek, ha voltak még egyáltalán), de nem ez a lényeg. Az eredmény jelentősége abban rejlik, hogy a bizonyítások egyre komplexebbé válásával a levezetések ellenőrzését nem tudjuk mindig mi magunk elvégezni. Eljöhet –egyesek szerint közel van már– az idő, amikor egy-egy bizonyítás ellenőrzése jelentősen nehezebb lesz, mint magának a bizonyításnak a megtalálása. De úgy tűnik, van remény, és nem fog emiatt megállni a tudomány: lehetőség lesz az ellenőrzés gépesítésére, hisz a ma ismert bizonyítások egyik legkomplexebbike esetében ez sikerrel megtörtént.

De térjünk vissza a próféciáktól az eredeti 4-szín tételre adott hibás bizonyításhoz. Kempe 11 évig megtévesztette a világot, ami szép teljesítmény, még ha nem szándékos. A hiba megtalálása után azonban a bizonyítás menthetetlennek tűnt. Az ott használt módszer azonban annyiból nem haszontalan, hogy alkalmas egy gyengébb, ám nemtriviális eredmény igazolásásra.

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

Biz.: Legfeljebb 3-pontú gráfokra a tétel triviálisan igaz. Nagyobb gráfokra 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.



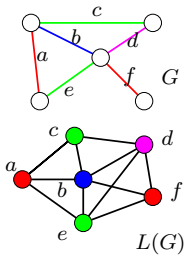
Mivel $G-v$ is egyszerű és síkbarajzolható, ezért az indukciós feltevés miatt 5-színezhető. Ha tehát v szomszédai legfeljebb 4 színt kapnak e színezésben, akkor v megkaphatja az ötödik színt. Ez akkor nem működik, ha $d(v) = 5$ és mind az öt szomszéd különböző színű[5]. (Ld. az ábrát.) Tekintsük az 1-es 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, Kempe mit nézett el, azaz, hogy a fenti bizonyítás miért is nem működik 4 színre.

1.2.1 Gráfok élszínezése

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 *élkromatikus száma* $\chi'(G) = \chi_e(G) = k$, 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 H 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 csúcs és annak v' másolata közé behúzunk további $\Delta(G) - d(v)$ párhuzamos élt.) 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.

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

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 $\chi'(G) \leq \Delta(G)+1$. □

Shannon tétele: Ha G véges, gráf, akkor $\chi'(G) \leq \frac{3}{2}\cdot\Delta(G)$. □

Megjegyzés: Ha egy K_3 minden élét k párhuzamos éllel helyettesítjük, akkor az így kapot G gráfra $\chi'(G) = \frac{3}{2}\cdot\Delta(G)$.

1.3 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.[6]

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. Minden fa (sőt erdő is) páros gráf, ezért egyúttal 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) $\omega(G) = \alpha(\overline{G}) = n - \tau(\overline{G}) = n - \nu(\overline{G})$. A $\chi(G) = \omega(G)$ egyenlőség igazolásához a triviális $\chi(G) \geq \omega(G)$ egyenlőtlenség miatt elegendő a $\chi(G) \leq \omega(G)$ bizonyítása, azaz G egy $\omega(G) = n - \nu(\overline{G})$ 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. □

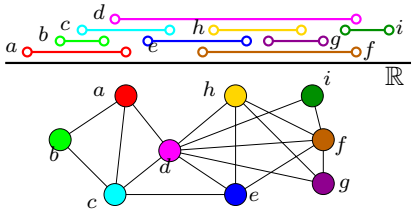
[6] Az egyenlőség persze magára a G gráfra is teljesül, de a vizsgán annyiszor hallottunk helytelen definíciót, hogy itt is igyeszünk hangsúlyozni, hogy nem csak az eredeti gráfra kívánjuk meg a leírt tulajdonságot.

A $\preceq$ relációt az X halmazon *részbenrendezésnek* nevezzük, ha létezik az X ponthalmazon egy aciklikus D irányított gráf, melyre $(x \preceq y) \iff (x \overset{D}{\longrightarrow} y)$. (Az x-t akkor tekintjük kisebbnek y-nál, ha x-ből irányított úton y-ba juthatunk.) 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 $\preceq := \overset{D}{\longrightarrow}$ 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 $\preceq = \overset{D}{\longrightarrow}$. 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 rendezés*.)
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 xy-k, melyekre $x \neq y$, továbbá x és y 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 $\preceq = \overset{D}{\longrightarrow}$. Jelölje V_i a G azon v csúcsainak halmazát, amire az igaz, hogy a v-ből induló leghosszabb D-beli irányított út pontosan i csúcsot tartalmaz. Mivel D aciklikus, ezért a definícióból adódik, hogy $V(G)$ a diszjunkt $V_1, V_2, \ldots, V_k$ halmazok uniója, és az is, hogy minden V_i halmaz független. Ezért $\chi(G) \leq k$. Másrészt, ha $x \in V_k$, akkor létezik egy x-ből induló, k pontú irányított út D-ben, és ezen út csúcsai egy k méretű klikkjét alkoltják a G gráfnak. Ezek szerint $\omega(G) \geq k \geq \chi(G)$, és ezt akartuk igazolni. □

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.

Az intervallumgráfok perfektségének közvetlen bizonyítása:
Figyeljük meg, hogy az intervallumgráf minden feszített részgráfja intervallumgráf, amit épp a feszített részgráf csúcsainak megfelelő intervallumok határoznak meg. Ezért elegendő azt igazolni, hogy tetszőleges

G intervallumgráfra $\chi(G) = \omega(G)$. Láttuk, hogy a $\chi(G) \geq \omega(G)$ egyenlőtlenség minden gráfra teljesül, ezért a feladatunk mindössze annyi, hogy a $\chi(G) \leq \omega(G)$ egyenlőtlenséget igazoljuk, azaz, színezzük ki G-t k színnel és ugyanakkor találjunk egy k méretű klikket is G-ben.

A G gráf kiszínezését a már látott mohó színezéssel végezzük, ahol a csúcsokat a megfelelő intervallumok balvégpontjainak növekvő sorrendjében vesszük. (Az ábrán látható intervallumgráf esetén ez az $abcdefhgi$ sorrendnek felel meg.) Tehát G csúcsait ebben a sorrendben színezzük úgy, hogy minden újabb intervallumnak megfelelő csúcs kiszínezésekor a legkisebb sorszámú olyan színt használjuk, ami nem okoz azonos színű végpontokkal rendelkező élt. Tegyük fel, hogy k színt használtunk fel eközben. Mit mondhatunk annak az x csúcsnak megfelelő intervallumról, amit a k-dik színre festettünk? Nos, x-nek vannak olyan $v_1, v_2, \ldots, v_{k-1}$ szomszédai, amiket korábban már az első $k-1$ színnel megszíneztünk. Ezek szerint a $v_1, v_2, \ldots, v_k$ intervallumok mindegyikének van közös pontja az x intervallummal. Az intervallumok feldolgozási sorrendjéből adódóan ez azt jelenti, hogy x bal végpontját minden egyes v_i intervallum tartalmazza, azaz, a $v_1, v_2, \ldots, v_{k-1}, x$ csúcsok G-ben egy k méretű klikket alkotnak. Nekünk pedig éppen ezt kellett bizonyítanunk. □

Az intervallumgráfok perfektségére adunk egy másik bizonyítást is a gyenge perfekt gráf tétel felhasználása nélkül, amivel általánosabb eredmény igazolható.

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 harmadik 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.

1.4 Hálózati folyamok és alkalmazásaik

A továbbiakban olyan irányított gráfokat vizsgálunk, melyek minden éléhez tartozik egy, az adott élt valamilyen szempontból jellemző szám. Számos gyakorlati probléma vezet ilyen számozott élekkel rendelkező gráfokra, elég itt az ebben a félévben nem tárgyalt (de az algoritmuselmélet keretében hamarosan részletesen megismert) legrövidebb utakra vagy a (szintén algelben felbukkanó) PERT problémára utalni. Mi itt most egy másik modellel foglalkozunk.

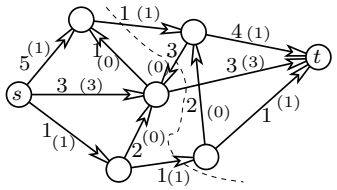
Def.: *Hálózatnak* nevezünk egy olyan (G, s, t, c) négyest, amelyben G egy irányított gráf, aminek s és t különböző csúcsai, továbbá G minden e élét jellemzi egy nemnegatív $c(e)$ szám, az e él ú.n. *kapacitása*[7].

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.[8]

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

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

Az 1. alatti *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.



Hálózati folyam. A zárójelekben az f folyam által felvett értékek állnak. A folyamérték $m_f = 1 + 3 + 1 = 5$. A szaggatott vonal 5 értékű vágást jelöl. (A Ford-Fulkerson algoritmus másikat talál.)

Def.: Az f folyam m_f *folyam nagysága* az a nettó 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 nagyságát máshogyan is kiszámíthatjuk.

Def.: 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 folyamnagyságra. Sőt, azt sem nehéz elhinni, hogy tetszőleges f folyam m_f folyam nagysága 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 $m_f \le \sum\{c(xv) : x \in X \not\ni v \in V(G)\}$.

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

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

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

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

[7] Nem követelmény, a G gráf aciklikussága: megengedünk irányított köröket is. Sőt: azt sem kívánjuk meg, hogy s forrás és t nyelő legyen, azaz futhat irányított él s-be ill. t-ből kifelé. Jegyezzük meg azonban, hogy néha szokás a hálózatot úgy definiálni, hogy ezen éleket megtiltjuk. E miatt nevezik időnként az s csúcsot a hálózatban *forrásnak* vagy *termelőnek*, t-t pedig *nyelőnek* vagy *fogyasztónak*. Helyesebb elnevezés talán s-t és t-t *terminális* csúcsoknak, a továbbiakat pedig *nemterminálisoknak* hívni. A vizsgán persze ezt sem kell tudni.

[8] 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 a szemléletes példa nagyjából ismeretével felvértezve vág neki a vizsgának, és nem képes definiálni az absztrakt fogalmakat (úgymint **hálózat, folyam, folyamnagyság,** st**-vágás** ill. **vágás kapacitása**). Tisztelettel szeretnék mindenkit lebeszélni az ilyesfajta próbálkozásról. *FT*

Az st-vágás tehát egy kézenfekvő eszköz annak bizonyítására, hogy a folyamnagyság nem lehet nagyobb egy adott mennyiségnél. Valójában ennél jobb bizonyíték nem is kell: a maximális folyamnagyság 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 folyamnagyság 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 folyamnagyságokra. A lehetséges folyamnagyságok x szuprémuma tehát véges. Azt kell megmutatni, hogy létezik x nagyságú 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 (régebbi nevén csendőr-szabály) 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 folyamnagyság definíciójából pedig az látszik, hogy $x = \lim m_{f_n} = \lim m_{f_{n_i}} = m_f$, tehát f csakugyan egy maximális folyam.

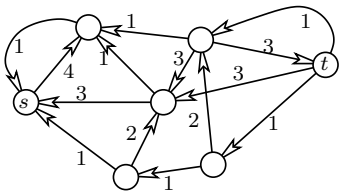
Legyen tehát f egy maximális folyam. A célunk f segítségével egy m_f kapacitású vágás megtalálása. Bevezetjük a (G_f, s, t, c_f) hálózatot a $G_f = (V(G), E_f)$ segédgráfon, melyre $E_f := E_f^{előre} \cup E_f^{vissza}$, ahol

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

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. (Ha egy konkrét élre mind a két feltétel teljesül, akkor azt előre- és visszaélként is bevesszük a segédgráfba.) 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 nagysága $m_{f'} = m_f + \varepsilon > m_f$, 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 folyamnagyságot 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. □

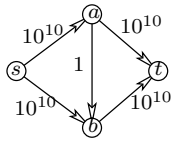
Ha a c kapacitások egészek, akkor a fenti bizonyítás egyben módszert is kínál a maximális folyam keresésére: kiindulunk az $f_0 \equiv 0$ folyamból, és elkészítjük az $f_0, f_1, f_2, \ldots$ folyamok sorozatát, melyekre $0 = m_{f_0} < m_{f_1} < m_{f_2} < \ldots$ egészek. Ha f_k-t már megtaláltuk, és 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 meghatározásához bizonyos $c_{f_k}(e)$ (pozitív egész) kapacitások minimumát kellett képezni. Tehát $m_{f_k} < m_{f_{k+1}}$, és az $m_{f_{k+1}}$ folyamnagyság is egész. Mivel a maximális folyamnagyságot 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. Ekkor ugyanis minden egyes javításkor legalább a kapacitások közös nevezőjének reciprokával növeljük a folyam nagyságát, amit nem tehetünk meg végtelen sokszor. 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} folyamnagyságok nem a maximális folyamnagysághoz, hanem egy annál kisebb számhoz konvergálnak. Egy másik kellemetlenség, hogy a fenti, növelő utas algoritmus sokszor sajnos nem elég hatékony. Az alábbi tétel mindkét problémára megoldást kínál.

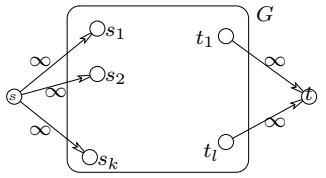
Edmonds-Karp tétel: Ha a (G, s, t, c) hálózatban a maximális folyamot a javítóutas algoritmussal keressük, és mindig egy legkevesebb élből álló javító út mentén növelünk, akkor a maximális folyam meghatározásához szükséges lépésszám felülről becsülhető $|V(G)|$ polinomjával. □

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

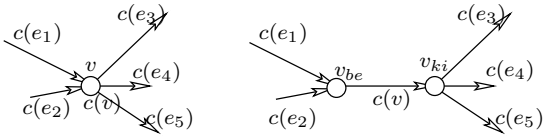


Ha eszetlenül próbálunk javítani, akkor indokolatlanul sok munkába kerülhet egy maximális folyam megtalálása: az ábrán látható hálózatban felváltva az *sabt* ill. *sbat* javító utakat választva mindig csak egységnyit tudunk emelni a folyamnagyságon, tehát az Edmonds-Karp algoritmus által két javítás után megtalált, $2 \cdot 10^{10}$ nagyságú 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[9]. 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.



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 nagyságú folyamot is a szovjet támaszpontokból Nyugat-Európába. A légicsapások tervezését elősegítendő, 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 kezelő specialisták mellett 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 feldolgozni a következő két fejezetet (a Menger tételek ill. páros gráfok párosításainak áttekintését), amik bár jóval korábbi eredmények, tárgyalásuk a hálózatok ismeretében sokkal egységesebb.

1.4.1 Menger tételei és gráfok többszörös összefüggősége

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. $V(P) \cap$

[9] 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_jt él kapacitása pedig legyen több annál, mint amennyi folyam t_j-be érkezhet az odavezető éleken.

$V(Q) = \{u, v\}$). Az éldiszjunkt (pontdiszjunkt) uv utak maximális számát $\lambda(u, v)$-vel (ill. $\kappa(u, v)$-vel) jelöljük.

Def.: Azt mondjuk hogy a G (irányított vagy irányítatlan) gráf U ponthalmaza (ill. F élhalmaza) *lefog* minden uv utat, ha a $G - U$ (ill. $G - F$) gráfban nem létezik u-ból v-be (irányított) út.

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 különböző, 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, nem szomszédos 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.

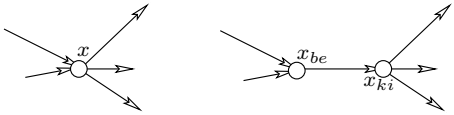
1. Definiáljuk a $(G, u, v, \mathbf{1})$ hálózatot. Ebben a hálózatban minden uv egészfolyam 0-t vagy 1-t rendel minden élhez. Legyen f ebben a hálózatban egy maximális nagyságú folyam, és legyen X olyan ponthalmaz, ami egy minimális uv-vágást határoz meg. Mivel minden él kapacitása egész, ezért az egészértékűségi lemma miatt feltehetjük, hogy f egészfolyam, és a nagysága mondjuk k. Ez itt azt jelenti, hogy G bármely élen vagy 0 vagy 1 mennyiségű folyam folyik. Az is igaz még, hogy az X ponthalmaz (ami u-t tartalmazza de v-t nem) olyan vágást határoz meg, aminek a kapacitása k. Ez itt azt jelenti, hogy X-ből pontosan k él lép ki. Világos, hogy ezt a k élt elhagyva nem tudunk az X halmazból $V \setminus X$-be eljutni, tehát ez a k él minden uv utat lefog, vagyis az uv utakat lefogó élek minimális száma legfeljebb k. A továbbiakban tehát nincs más célunk, mint azt megmutatni, hogy létezik k éldiszjunkt uv út G-ben.

Megjegyzés: Az f maximális egészfolyamra gondolhatunk úgy, mint a javító utas algoritmus által szolgáltatott folyamra, hiszen egész kapacitások esetén az bizonyosan minden élen egész értéket vesz fel. Mivel minden él kapacitása egységnyi, ezért minden egyes javító út pontosan egy egységnyivel javította az aktuális folyamot, tehát a javító utas algoritmus pontosan k javító utat használt f konstrukciójában. Csábító gondolat, hogy ezzel készen is vagyunk, hiszen *„a k javító útnak az egységnyi kapacitások miatt muszáj éldiszjunktnak lennie, ezért máris megtaláltuk a keresett k éldiszjunkt uv utat”*. Sajnos azonban ez a következtetés hibás, de szerencsére nem menthetetlenül. Ha mondjuk valami kozmikus szerencse folytán az f folyam konstrukciójában minden növelő út csak előreélekből állt, akkor helyes a következtetés. Ha azonban a növelő utakban visszaélek is szerepeltek, akkor még akár az a furcsaság is megtörténhet néhány növelés után, hogy a folyamban keletkezik egy minden mástól diszjunkt irányított kör, ahol pozitív mennyiségű folyam áramlik körbe, ám sem a körbe befelé, sem a körből kifelé nem folyik semmi. Amit az alábbiakban bebizonyítunk, az voltaképpen az, hogy tetszőleges f folyamhoz létezik olyan f' folyam, ami f-fel azonos nagyságú, minden élkapacitást legfeljebb annyira használ ki, mint f, ráadásul f' megkapható a növelő utas algoritmussal úgy, hogy mindig csak előreéleket használunk.

Tekintsük tehát a fent definiált, k nagyságú f folyamot, és legyen E' a G azon éleinek halmaza, amiken 1 egységnyi folyam folyik. A Kirchoff-szabály miatt minden u-tól és v-től különböző w csúcsra igaz, hogy E'-nek pontosan annyi éle mutat w-be, mint amennyi E'-beli él kilép w-ből. Abból pedig, hogy f nagysága k az következik, hogy u-ból k-val több E'-beli lép ki, mint amennyi u-ba érkezik, v-be pedig éppen k-val több éle érkezik E'-nek, mint amennyi kilép belőle. Tekintsük a $G^* = (V, E^*)$ gráfot, ahol az E^* élhalmazt úgy kapjuk, hogy E'-höz hozzáveszünk még k párhuzamos vu élt. A G^* gráf konstrukciója folytán G^* minden csúcsának megegyezik a kifoka és a befoka. Legyen K a G^*-nak az az irányítatlan értelemben vett komponense, ami az u csúcsot tartalmazza. A vu élek bevétele miatt K tartalmazni fogja persze a v csúcsot is. Az Euler-körsétákról szóló tétel irányított változata szerint K-nak létezik Euler-körsétája. Ha ebből a körsétából elhagyjuk az utólag bevett k párhuzamos vu élt, akkor a körséta k *éldiszjunkt* irányított uv sétára esik szét. Minden ilyen uv sétából (esetleges körök elhagyása után) kiválasztható egy-egy irányított uv út.

Azt kaptuk tehát, hogy létezik k éldiszjunkt irányított uv út és egyúttal k éllel lefogható minden irányított uv út G-ben. Ezért az éldiszjunkt irányított uv utak maximális száma legalább annyi, mint az összes irányított uv utat lefogó élek minimális száma. A triviális max $\leq$ min egyenlőtlenséggel ezt egybevetve éppen a Menger tétel 1. része adódik.

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.



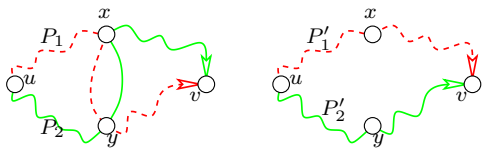
Ha ezt G minden $x \neq u, v$ csúcsára elvégezzük, akkor az így kapott G' gráfban k éldiszjunkt uv út

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 nagyságú *egész*folyamból, a minimális lefogó halmaz pedig egy minimális kapacitású 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, hamarosan sorra kerülő $\nu = \tau$ 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. Ám, hogy hogyan, azt nem árulta el. Az említett könyvben valóban egy helyes bizonyítás szerepel, de Menger egy szóval sem említi, hogy az eredeti bizonyítása hiányos. És természetesen Kőnig nevét is hiába keresnénk ennél a résznél.

A Menger tétel Ford-Fulkerson alapú bizonyításához nem használtuk fel Kőnig tételét, ellentétben az eredeti bizonyítással, amihez szükség volt arra. Érdemes azonban látni e két tétel kapcsolatát is, ezért a következő szakaszban levezetjük a Kőnig tételt Menger eredeti tételéből (És igen: a vizsgán ezt is elfogadjuk az ott közölt bizonyítás helyett.)

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 él 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. □

1.4.2 Párosítások és gráfparaméterek

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.

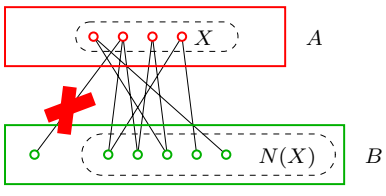
Példa: Egy tánciskolában tanuló fiúk ill. lányok halmazai alkossák a G páros gráf színosztályait. Fusson G-ben él két csúcs között, ha az adott fiú és lány hajlandó egymással táncolni. Ekkor G minden párosítása egy lehetséges táncpartner-választási szituációt ír le. Ebben a modellben a hatékony oktatás 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 $\nu(G) \leq \tau(G)$. (Itt G nem feltétlenül páros gráf.)

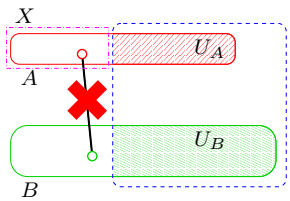
Biz.: Legyen M G-nek egy maximális ($\nu(G)$ élből álló) párosítása. Ha U egy minimális méretű lefogó ponthalmaz, akkor lefogja M minden élét is, ám U minden pontja legfeljebb egy párosításélt fog le. Tehát $\tau(G) = |U| \geq |M| = \nu(G)$. □

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

Történelem Frobenius 1912-ben publikált egy determinánsokra vonatkozó eredményt, ami a gráfok nyelvén fogalmazva a páros gráfok teljes párosításának jellemzésével egyenértékű. Kőnig 1915-ben ettől az eredménytől függetlenül bizonyította a szóbanforgó tételét, amit aztán elküldött Frobeniusnak. Frobenius később megjelentetett egy elemi bizonyítást a saját tételére, majd ugyanitt úgy említette Kőniget, mint akinek az eredménye könnyen következik az övéből. Mindezen túl azt is megjegyezte, 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, megtalálható az ő saját, determinánsokról szóló tételében". Nos, az idő nem Frobeniust igazolta.

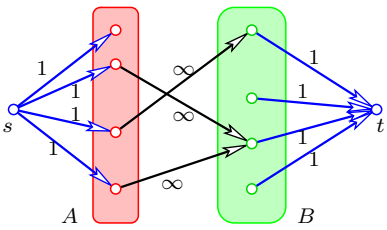
A Hall tétel bizonyítása: A szükségesség nyilvánvaló: ha létezik A-t fedő párosítás, akkor minden A-beli pontnak különböző párja van, tehát tetszőleges $X \subseteq A$ esetén az X-beli elemek B-beli párjai az $N(X)$ egy $|X|$ méretű részhalmazát alkotják.

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. a Hall feltétel miatt



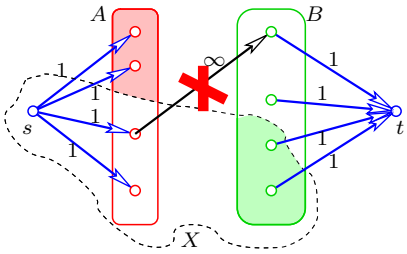
$$\nu(G) = \tau(G) = |U| = |U_A| + |U_B| \geq |U_A| + |N(X)| \geq |U_A| + |X| = |A| \ .\square$$

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 nagyságú 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 $\nu(G)$ kapacitású 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. $\square$



A Kőnig tétel iménti bizonyításából hatékony algoritmust kaphatunk egy páros gráf maximális párosításának ill. minimális lefogó ponthalmazának megtalálására. Ha ugyanis a maximális folyamok meghatározására szolgáló javító utas módszert a fenti konstrukcióra alkalmazzuk, és eltekintünk az s-re ill. t-re illeszkedő élektől, akkor az alábbi eljárás adódik. 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 $M \Delta P$-t 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 bizonyítása Menger tételével: 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 pontdiszjunkt 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 Néha –helytelenül– a fent ismertetett eljárást nevezik *magyar módszernek*. Az „igazi" 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, pinduri 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 háromjegyű élsúlyokkal rendelkező, 24 csúcsú páros gráfon egy maximális súlyú párosítását. Mivel ehhez mindössze 3 órára volt szüksége, ez 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. Egyedül ezzel a nagylelkű gesztussal Kuhn valószínűleg jóval többet tett a hazai matematika nemzetközi elismertségéért, mint Frobenius és Menger együttvéve.

A továbbiakban nem feltétlenül páros gráfok párosításait, illetve a párosítások szempontjából hasznos paramétereit vizsgáljuk.

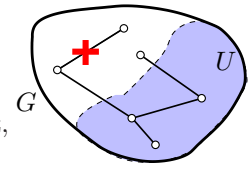
Def.: A G gráf pontjainak U részhalmaza *független* (vagy *stabil*), ha U nem feszít élt, azaz G minden élének van nem U-beli végpontja. A G gráf legtöbb pontból álló, független ponthalmazának méretét $\alpha(G)$ jelöli.

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.

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 $\rho(G) \leq n - \nu(G)$, ahonnan $\nu(G) + \rho(G) \leq n$ 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 $\nu(G) \geq k$. Azt kaptuk, hogy $\rho(G)+\nu(G) \geq n-k+k = n$, 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: $\alpha(G) = |V(G)| - \tau(G) = |V(G)| - \nu(G) = \rho(G)$. □

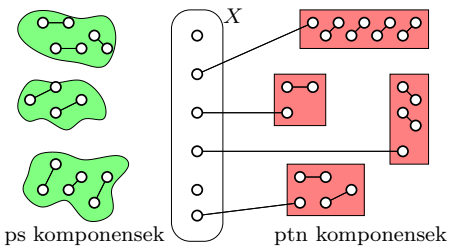
A maximális párosítás méretének (azaz a $\nu(G)$ gráfparaméternek) a meghatározása nem csak páros gráfok esetén érdekes. Ezért hasznos megfigyelés, hogy a javító alternáló utakkal való növelés (elméletileg) itt is maximális párosítást ad. (A páros gráfokon használt alternáló ill. javító út fogalma értelemszerűen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

1.5 Gráfok mátrixai

Def.: A $G=(V,E)$ (irányított) gráf *szomszédsági (adjacencia) mátrixa* $A(G) = (a)_{i,j} \in \mathbb{R}^{V\times V}$, ahol $a_{i,j} :=$ az i-ből j-be futó élek száma.

Megfigyelés: Ha G (irányított) gráf, akkor v pontjának (ki)-foka az $A(G)$ mátrix v-hez tartozó sorában levő elemek összege. A v-hez tartozó oszlopösszeg a v (be)-foka. Ha G irányítatlan, akkor $A(G)$ szimmetrikus: $A(G) = A(G)^T$.

Tétel: Ha $G=(V,E)$ (irányított) gráf, akkor az A^k mátrix (u,v) pozícióban álló $(A^k)^v_u$ eleme megegyezik az u-ból v-be vezető, k élű séták számával.

Biz.: Teljes indukcióval: $k=$ 1-re ez $A(G)$ definíciójából közvetlenül következik. Tegyük fel, hogy $A(G)^k$-ra már bizonyítottuk az állítást. Világos, hogy az u-ból v-be vezető $(k+1)$-élű séták száma $\sum_{w\in V}($ a k élű uw séták száma$)\cdot($ a wv élek száma$) = \sum_{w\in V}(A(G)^k)^w_u \cdot A(G)^v_w = (A(G)^{k+1})^v_u$, ahol az első egyenlőség az indukciós feltevésből, míg a második a mátrixok szorzásának definíciójából adódik.□

Köv.: Ha G egyszerű, irányítatlan gráf, akkor $(A(G)^2)^v_v = d(v)\ \forall v \in V(G)$. □

Tétel: Ha G irányítatlan gráf, és λ_1 az $A(G)$ legnagyobb sajátértéke, akkor $\lambda_1 \leq \Delta(G)$, továbbá ha G Δ-reguláris, akkor $\Delta = \lambda_1$. (Emlékeztetünk, hogy $\Delta(G)$ a legnagyobb G-beli fokszámot jelöli.)

Biz.: Legyen $\underline{x} = (x_1, x_2, \ldots, x_n)$ egy λ_1-hez tartozó sajátvektor, és legyen $x_k = \max\{x_1, x_2, \ldots, x_n\}$. Mivel $\underline{x} \neq \underline{0}$, ezért (esetleg a $-\underline{x}$ sajátvektorra áttérve) feltehető, hogy $x_k > 0$. Ekkor $\lambda_1 \cdot x_k = A(G)_k \cdot \underline{x} = \sum_{i=1}^n a_{k,i}x_i \leq \sum_{i=1}^n a_{k,i}x_k = x_k \cdot \sum_{i=1}^n a_{k,i} = x_k \cdot d(v_k) \leq \Delta \cdot x_k$.

Másrészt, ha G Δ-reguláris, akkor $\underline{1}$ a Δ sé-hez tartozó sv, ugyanis a fenti egyenlőtlenségek végig egyenlőséggel teljesülnek. □

Def.: A $G=(V,E)$ irányított gráf *illeszkedési (incidencia) mátrixa* $B(G) \in \mathbb{R}^{V\times E}$, amire

$$(B(G))^e_v = \begin{cases} 1 & \text{ha } v \text{ az } e \text{ kezdőpontja} \\ -1 & \text{ha } v \text{ az } e \text{ végpontja} \\ 0 & \text{egyébként ,} \end{cases} \qquad \text{irányítatlanra} \quad (B(G))^e_v = \begin{cases} 1 & \text{ha } v \text{ az } e \text{ végpontja} \\ 0 & \text{egyébként.} \end{cases}$$

Tétel: A G irányított gráf $B(G)$ illeszkedési mátrixának néhány oszlopa pontosan akkor lineárisan független, ha a megfelelő élek irányítatlan megfelelői erdőt alkotnak.

Biz.: Egy körnek megelelő oszlopvektorok megfelelő, ± 1 együtthatókkal vett lineáris kombinációja a nullvektort adja, ezért minden független oszloprendszer erdőnek felel meg.

Ha egy oszloprendszer erdőnek felel meg, akkor egy tetszőleges, levélből induló él független a többi oszloptól, hisz a levélhez tartozó koordinátában a többi oszlop 0, a vizsgált oszlop pedig nem. Ezen él elhagyásával egy kisebb erdőt kapunk; ennek éleihez tartozó oszlopokról pedig indukcióval bizonyítható, hogy a lineárisan függetlenek. □

Köv.: Ha G irányított, hurokélmentes, n-pontú gráf c komponenssel, akkor $r(B(G)) = n - c$.

Biz.: $B(G)$ rangja azonos $B(G)$ oszloprangjával, azaz feszítő erdejének élszámával, ami $n-c$. □

Tétel: Ha B a G gráf $B(G)$ illeszkedési mátrixából egy sor elhagyásával keletkező mátrix, akkor $\det(BB^T)$ a G feszítőfáinak száma.

A bizonyításhoz szükséges az alábbi, a determinánsok szorzástételét általánosító segédtétel.

Lemma: (Binet-Cauchy tétel) Ha $M \in \mathbb{R}^{[n]\times[m]}$, $N \in \mathbb{R}^{[m]\times[n]}$ és $n \leq m$, akkor $\det(M\cdot N) = \sum_{H\in\binom{[m]}{n}} \det(N^H)\cdot \det(M_H)$, ahol N^H az N mx H-beli oszlopai, M_H pedig az M mx H-beli sorai meghatározta részmátrix. □

A B mátrix oszlopainak egy részhalmazát pontosan akkor alkot reguláris mátrixot (az előző tétel szerint), ha az adott oszlopok egy feszítőfának felelnek meg. Ekkor pedig a determináns ± 1, u.i. pontosan egy nemnulla kifejtési tag van. (Az elhagyott sornak megfelelő pontot gyökérnek tekintve, minden oszlophoz azt a sort választjuk, ami az oszlopnak

megfelelő él gyökértől távolabbi végpontjához tartozik.) A B^T mátrix ugyanezen *sor*részhalmazhoz tartozó részmátrixának a determinánsa ugyanannyi, ezért $H \in \binom{E}{n-1}$-re

$$\det(B^H) \cdot \det(B_H^T) = \begin{cases} 1 & \text{ha } H \text{ feszítőfa} \\ 0 & \text{ha } H \text{ nem feszítőfa} , \end{cases}$$

ezért a Binet-Cauchy tétel miatt $\det(B \cdot B^T)$ csakugyan G feszítőfáinak száma. □

Köv.: Cayley tétel: A K_n gráfnak n^{n-2} feszítőfája van.

Biz.: A az előző tétel szerint BB^T mátrix determinsa adja a feszítőfák számát, ahol a B a mátrix úgy keletkezik, hogy a $B(K_n)$ illeszkedési mátrixból egy sort elhagyunk. A mátrixszorzás definíciója miatt a $(BB^T)_v^v = d(v) = n-1$, ill. $u \neq v$-re $(BB^T)_v^u = d(v) = -1$. Így

$$\begin{vmatrix} n-1 & -1 & \dots & -1 \\ -1 & n-1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & -1 \\ -1 & \dots & -1 & n-1 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ -1 & n-1 & -1 & \dots & -1 \\ -1 & \ddots & n-1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & -1 \\ -1 & \dots & \dots & -1 & n-1 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & n & 0 & \dots & 0 \\ 0 & \ddots & n & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & n \end{vmatrix} = n^{n-2} \qquad \square$$

2. fejezet

Számelmélet

2.1 Oszthatóság, prímek, közös osztók

Def.: Az a, b egész számokról azt mondjuk, hogy a *osztja* b-t, illetve b az a *többszöröse*, (jelölése $a \mid b$), ha $b = aq$ valamely q egész számra. Világos, hogy $n \neq 0$ esetén $\pm 1, \pm n \mid n$, ezek az n *triviális osztói.* Az n azon osztóit, amelyek nem triviálisak, *valódi osztóknak* nevezzük.

Példa: $1 \mid -7, 19 \mid 0, -3 \mid 9, 0 \nmid 2, 0 \mid 0$.

Def.: A $p \in \mathbb{Z}$ szám *felbonthatatlan* (néha *irreducibilis*, ómagyarul *törzsszám*), ha $|p| \neq 1$ és p-t csak triviális módon tudjuk egészek szorzataként előállítani, azaz $p = ab$ $(a, b \in \mathbb{Z})$ esetén $|a| = 1$ vagy $|b| = 1$. Ugyanezt úgy is mondhatjuk, hogy p akkor felbonthatatlan, ha p-nek csak triviális osztói vannak[1], és $p \neq 1$ ill. $p \neq -1$.[2]

Példa: $2, -5, 11$ felbonthatatlanok, a -1 ill. a $-9 = 3 \cdot (-3)$ pedig nem azok.

Megjegyzés: Korábban azt tanították, hogy a most definiált számok a prímszámok. Ez így nem pontos. Látni fogjuk, hogy a prímek definíciója egészen más, mint a felbonthatatlanoké. Jóllehet, az egészek körében a két fogalom azonos számhalmazt definiál, a felbonthatatlan és prím tulajdonság más „számkörökben" értelmezve, nem feltétlenül ugyanazt jelenti. A lényeg, amire itt rá szeretnék mutatni, hogy tudjunk arról, hogy más a prím és más a felbonthatatlan definíciója, és korántsem triviális, hogy egészek körében a két fogalom egybeesik.

Állítás: Bármely z egész szám előáll felbonthatatlan számok szorzataként ha $|z| > 1$.

Biz.: $|z|$ szerinti teljes indukciót alkalmazunk. Világos, hogy $|z| = 2$ esetén z felbonthatatlan, és mint egytényezős szorzat megfelel. Tegyük fel, hogy k-ig már bizonyítottunk, azaz minden olyan számra igaz a tétel, aminek az abszolút értéke legfeljebb k. Legyen $|z| = k + 1$. Ha z felbonthatatlan, akkor z megfelel, mint egy egytényezős szorzat. Ha z nem felbonthatatlan, akkor z nemtriviális módon felbomlik $z = ab$ alakban, ahol $1 < |a| \leq k$ és $1 < |b| \leq k$. Az indukciós feltevés értelmében a és b is előáll felbonthatatlan számok szorzataként, ezért ez a szorzatukra, z-re is igaz. □

A számelmélet alaptétele: Ha egy z egész számra $|z| > 1$, akkor z előáll felbonthatatlan számok szorzataként, és a z ilyen előállításai csak a tényezők sorrendjében és előjeleiben különbözhetnek.

Példa: A -24 néhány lehetséges előállítása $-24 = 2 \cdot 3 \cdot (-2) \cdot 2 = (-3) \cdot (-2) \cdot (-2) \cdot 2 = (-2)^3 \cdot 3$, és ezek csakugyan az előjelekben és a sorrendben különböznek csupán.

Def.: Az $1 < n \in \mathbb{N}$ szám *kanonikus alakján* egy olyan $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ előállítást értünk, amiben $p_1, p_2, \ldots, p_k$ különböző (pozitív) felbonthatatlanok és az $\alpha_1, \alpha_2, \ldots, \alpha_k$ számok pedig pozitív egészek. Időnként szokás azt is feltenni, hogy $p_1 < p_2 < \ldots < p_k$.

Az imént bizonyított állítás miatt minden 1-nél nagyobb egésznek létezik kanonikus alakja és ez a kanonikus alak a számelmélet alaptétele szerint a sorrendtől eltekintve egyértelmű.

A számelmélet alaptétele nem axióma. Bármennyire is magától értetődőnek érezzük (elsősorban az általános- és középiskolás súlykolás miatt), bizonyításra szorul. Az alábbi bizonyítás egyúttal arra is rámutat, hogy mi az az ok, ami miatt az egészek alkotta számkörben igaz a tétel.

A számelmélet alaptételének bizonyítása: A már bizonyított állítás szerint a vizsgált számok előállnak felbonthatatlanok szorzataként. Mivel egy szám pontosan akkor felbonthatatlan, ha az ellentettje felbonthatatlan, elegendő pozitív egészekre szorítkoznunk a bizonyításban. A felbontás egyértelműségéhez tehát csak azt kell igazolni, hogy ha $z = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_l$ két előállítás,

[1] Helytelenül ezt úgy szokás mondani, hogy p-nek csak az 1 és önmaga az osztója. Helyesen: csak a ± 1 és a $\pm p$.

[2] Időnként ez is kimarad a definícióból.

amelyekre $p_1 \le p_2 \le \ldots \le p_k$ és $q_1 \le q_2 \le q_l$, teljesül, akkor $k = l$ és a $p_i = q_i$ minden i-re. Ezt is z szerinti teljes indukcióval bizonyítjuk. Ha $z = 2$, akkor z felbonthatatlan, nincs mit igazolunk. Tegyük fel tehát, hogy a z-nél kisebb számokra már megmutattuk a felbontás egyértelműségét. Tekintsük a fenti $z = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_l$ felbontásokat. Az általánosságot az sem korlátozza, ha kikötjük, hogy $p_1 \le q_1$.

I. eset: $p_1 = q_1$. Ekkor $\frac{z}{p_1} = p_2 \cdot p_3 \cdot \ldots \cdot p_k = q_2 \cdot q_3 \cdot \ldots \cdot q_l$. Mivel $\frac{z}{p_1} < z$, az indukciós állítás szerint $k = l$ és $p_2 = q_2, p_3 = q_3, \ldots, p_k = q_l$. Így $p_1 = q_1$ miatt z-re is igaz az indukciós állítás.

II. eset: $p_1 < q_1$.

Ekkor

$$z = p_1 \cdot p_2 \cdot \ldots \cdot p_k = (q_1 - p_1) \cdot q_2 \cdot \ldots \cdot q_l + p_1 \cdot q_2 \cdot \ldots \cdot q_l,$$

tehát

$$p_1(p_2 \cdot p_3 \cdot \ldots \cdot p_k - q_2 \cdot q_3 \cdot \ldots \cdot q_l) = (q_1 - p_1) \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_l =: z' \ .$$

Világos, hogy $z' < z$, ezért z'-re tudjuk, hogy igaz a számelmélet alaptétele. A fenti két felírás alapján elkészíthetjük a z' felbonthatatlanok szorzataként történő kétféle felírását, mégpedig úgy, hogy a bal oldalon a $(p_2 \cdot p_3 \cdot \ldots \cdot p_k - q_2 \cdot q_3 \cdot \ldots \cdot q_l)$, a jobb oldalon pedig a $(q_1 - p_1)$ tényezőt helyettesítjük egy-egy felbonthatatlanok szorzatáként történő előállításukkal. E két felírásból a bal oldalon p_1 lesz az egyik tényező, így az indukciós feltevés szerint p_1-nek szerepelnie kell a jobb oldalon is. Mivel p_1 mindegyik q_i-nél kisebb ezért p_1-nek az $(q_1 - p_1)$ felbontásában kell szerepelnie. Ekkor azonban $p_1 \mid q_1 - p_1$, ezért $p_1 \mid q_1$, és ez $1 < p_1 < q_1$ miatt ellentmond q_1 felbonthatatlanságának. Az ellentmondás azt mutatja, hogy a II. eset nem valósulhat meg, és ezzel az indukciós bizonyítást befejeztük. □

Megjegyzés: Min múlik a fenti bizonyítás? A kulcs a II. eset gondolatmenete. Itt van ugyanis szükségünk a számhalmazunkon a természetes rendezésre. Lényegében azt mutatjuk ugyanis meg, hogy ha van egy olyan szám, amire a felbontás nem egyértelmű, akkor van egy másik ilyen szám is, és ez a másik *kisebb*, mint amit épp vizsgálunk. Más szóval bármely „rossz" számnál van kisebb „rossz" szám is, ami természetes számokon lehetetlenség.

A bizonyítás lelke tehát a számkör „természetes rendezése". Ennek a rendezésnek pontosan arra a tulajdonságára van szükségünk, amiből az is következik, hogy van „maradékos osztás", azaz minden $a \ge b$ esetén létezik egy $a = q \cdot b + m$ felírás, ahol $0 \le m < b$. Ezért a fenti bizonyítás minden olyan struktúrában elmondható, ahol van maradékos osztás. A felbonthatatlanság definíciójának értelemszerű módosításával a számelmélet alaptétele igaz marad pl. az ú.n. *Gauss-egészekre*, azaz az $a + bi$ alakú komplex számokra, ahol $a, b \in \mathbb{Z}$ és az egész együtthatós polinomok körében, jóllehet ez utóbbi struktúrában nincs maradékos osztás.

Itt az ideje, hogy végre megtudjuk mik is a prímek.

Def.: A $p \in \mathbb{Z}$ szám *prím*, ha tetszőleges $a, b \in \mathbb{Z}$-re teljesül, hogy $p \mid ab \Rightarrow p \mid a$ vagy $p \mid b$.

Szavakban: egy szám akkor prím, ha csak úgy tud osztani egy szorzatot, ha a szorzat valamelyik tényezőjét osztja. A számelmélet alaptételének fontos következménye a prím és a felbonthatatlan ugyanazokat a számokat jelenti.

Köv.: 1. Ha a p egész szám prím, akkor p felbonthatatlan.
2. Ha a p egész szám felbonthatatlan, akkor p prím.

Biz.: 1. Tegyük fel, hogy p prím és tegyük fel, hogy felbomlik $p = a \cdot b$ alakban. Ekkor persze $p \mid ab$, így a prímtulajdonság miatt $p \mid a$ vagy $p \mid b$, és az általánosság megszorítása nélkül feltehető, hogy $p \mid a$. Ekkor azonban $a = p \cdot k$ és $p \ne 0 \ne a$ miatt $|p| \le |a| \le |a| \cdot |b| = |ab| = |p|$ következik, tehát végig egyenlőség áll, vagyis $a = \pm p$. Így p bármely felbontása triviális, azaz p felbonthatatlan. Figyeljük meg, hogy ez az állítás független volt a számelmélet alaptételétől.

2. Most tegyük fel azt, hogy p felbonthatatlan és $p \mid ab$. Mivel $z = \frac{ab}{p}$ egész, ezért z-nek egy felbonthatatlanok szorzataként történő előállítását p-vel megszorozva az ab egy felbonthatatlanok szorzataként való előállítását kapjuk. A számelmélet alaptétele szerint ekkor a $\pm p$ tényezőnek az ab tetszőleges olyan szorzattábontásában szerepelni kell, ahol a tényezők felbonthatatlanok. Speciálisan abban a felbontásban is, amit úgy kapunk, hogy vesszük az a ill. a b egy-egy felbonthatatlanok szorzataként történő előállítását, és ezeket összeszorozzuk. Ezek szerint tehát p szerepel az a vagy a b felbonthatatlanok szorzataként történő előállításában, így $p \mid a$ vagy $p \mid b$. Ez pedig éppen a p prímtulajdonságát igazolja. □

Megjegyzés: Általában is igaz, hogy ahol igaz a számelmélet alaptétele, ott a prímek és a felbonthatatlanok ugyanazok. Mivel mind a Gauss-egészek, mind az egész együtthatós polinomok részstruktúraként tartalmazzák $\mathbb{Z}$-t, érdekes megvizsgálni, mik az ottani prímek. Az egész együtthatós polinomok körében a prímeket *irreducibilisnek* szokás nevezni. A 0-fokú irreducibilis polinomok éppen a szokásos prímek, de irreducibilis pl a $2x + 7$ vagy az $x^2 - 3x + 1$ is. A Gauss egészek körében viszont az az érdekesség is előfordul, hogy egy egész prím nem Gauss-prím. Pl. $2 = (1 + i)(1 - i)$ vagy $5 = (2+i)(2-i)$. Egész pontosan minden $4k+3$ alakú prím Gauss-prím is, de az összes többi prím két konjugált Gauss-prím szorzatára bontható.

A valós ill. a komplex együtthatós polinomok olyan további struktúrák, amikben van maradékos osztás, így igaz a számelmélet alaptétele. Láttuk, hogy a $p(x) = x^2 - 3x + 1$ irreducibilis az egészek felett. Ugyanez a polinom a valósak felett felbomlik két gyöktényező szorzatára $p(x) = (x - \alpha_1)(x - \alpha_2)$ alakban, ahol α_1 és α_2 a két gyöke a p polinomnak, és e gyöktényezők nyilván nem bonthatók további polinomok szorzatára nemtriviális módon. Az algebra alaptétele (miszerint minden n-edfokú polinomnak (multiplicitással számolva) pontosan n komplex gyöke van) úgy is fogalmazható, hogy a

komplex együtthatós polinomok között a prímek pontosan az első fokú polinomok. (Ez a gyöktényezők kiemelhetőségéből látszik.)

A valós együtthatós $x^2 - 3x + 4$ polinomnak nincs valós gyöke, ezért irreducibilis a valós együtthatós polinomok körében. Persze nem az a komplex együtthatósok között, ahol az elsőfokúak a prímek. Mivel egy valós együtthatós p polinom minden komplex gyökének a konjugáltja is gyök, ezért a két gyöktényező szorzata (ami egy másodfokú valós együtthatós polinom) irreducibilis faktora lesz a p polinomnak. Ebből az következik, hogy a valós együtthatós polinomok körében a prímek az elsőfokú és a valós gyökkel nem rendelkező másodfokú polinomok.

Természetesen az apróbetűs részt nem kell tudni a vizsgán. De abban reménykedek, egyeseknek talan nem érdektelen, ha a matematika viszonylag távolinak tűnő területei között kapcsolatot látnak. A többiektől elnézést kérek. FT

A számelmélet alaptétele által biztosított kanonikus alak segítségével jellemezhető az oszthatóság.

Állítás: A $d \in \mathbb{N}$ szám pontosan akkor osztója a $n \in \mathbb{N}$ számnak, ha d kanonikus alakjában kizárólag n kanonikus alakjában megtalálható prímek szerepelnek, és minden ilyen p_i prím kitevője legfeljebb annyi d-ben, mint n-ben.

Biz.: Ha $d \mid n$, akkor $n = d \cdot d'$ valamely d' egészre. Az n kanonikus alakját úgy kapjuk, hogy összeszorozzuk d és d' kanonikus alakját, vagyis a szükséges feltétel teljsesül. Az elégségesség igazolásához tegyük fel, hogy a kanonikus alakok az állításban leírt tulajdonsággal rendelkeznek, azaz $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ és $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$, és $\beta_i \leq \alpha_i$. Ekkor $n = d \cdot p_1^{\alpha_1-\beta_1} \cdot p_2^{\alpha_2-\beta_2} \cdot \ldots \cdot p_k^{\alpha_k-\beta_k}$, tehat $d \mid n$. □

Innen aztán remekül kiszámíthatjuk egy szám osztóinak számát a kanonikus alak segítségével.

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

Biz.: Bármely $d \mid n$ osztó kanonikus alakja olyan, hogy azt alkalmas 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.: Legyen $a, b \in \mathbb{Z}$ olyan, hogy $a \neq 0$ vagy $b \neq 0$ teljesül. Az a és b számok (a, b)-vel jelölt *legnagyobb közös osztója* a legnagyobb olyan szám, mely osztója a-nak és b-nek is.
Az a, b számokat *relatív prímnek* mondjuk, ha $(a, b) = 1$.

Az $a, b \in \mathbb{Z}$ számok legkisebb közös többszöröse az a legkisebb $n \in \mathbb{N}$ szám, amire $a \mid n$ és $b \mid n$ áll. Jelölése: $[a, b]$.

Példa: $(15, 24) = 3$, $(-22, 18) = 2$, $(-20, 0) = 20$ és $(0, 0)$ nem értelmezett, hisz a közös osztók $\mathbb{Z}$ halmazának nincs legnagyobb eleme. $[-5, -17] = 85$, $[-9, 0] = 0$ és $[0, 0] = 0$.

Az osztók kanonikus alakjára vonatkozó állítás segítségével könnyen kiszámíthatjuk a legnagyobb közös osztót ill. a legkisebb közös többszöröst.

Állítás: Ha $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ ill. $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_k^{\beta_1}$ (ahol $\alpha_i = 0$ és $\beta_i = 0$ is megengedett), akkor

$$(a, b) = p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdot \ldots \cdot p_k^{\min(\alpha_k,\beta_k)} \text{ ill.} [a, b] = p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdot \ldots \cdot p_k^{\max(\alpha_k,\beta_k)},$$

más szóval a lnko-hoz a kanonikus alakokban szereplő közös prímeket kell a kisebb hatványon, a lkkt-höz pedig a kanonikus alakokban szereplő valamennyi prímet a nagyobb hatványon kell összeszorozni.
Tetszőleges a, b pozitív egészekre $ab = (a, b) \cdot [a, b]$.

Biz.: Ha d közös osztó, akkor d kanonikus alakjában csak az a és b kanonikus alakjában szereplő közös prímek szerepelhetnek, legfeljebb a kisebbik kitevőn, ezért az lnko-ra adott képlet helyes. A lkkt-nek a és b is osztója, ezért a kanonikus alakban minden a-ban vagy b-ben előforduló prímnek legalább az a ill. b-beli kitevőn kell szerepelnie, ez pedig a második képletet indokolja.

A szorzatra vonatkozó azonosság azért igaz, mert minden prím ugyanazon a hatványon szerepel a jobb- ill. baloldal kanonikus alakjában. □

Ha a kanonikus alak nincs kéznél, akkor is boldogulhatunk a legnagyobb közös osztóval.

Állítás: Ha a és b egészek, akkor $(a, b) = (a - b, b)$.

Biz.: Tegyük fel, hogy d az a és b közös osztója, azaz $d \mid a$ és $d \mid b$. Ekkor $d \mid a - b$, azaz d az $a - b$-nek és a b-nek is közös osztója. Ha pedig d az $a - b$-nek és a b-nek is közös osztója, azaz $d \mid a - b$ és $d \mid b$, akkor $d \mid a - b + b = a$, tehát d ekkor az a-nak és a b-nek is közös osztója.

Azt kaptuk, hogy ugyanazok a számok lesznek az a és b közös osztói, amik az $a - b$-nek és a b-nek közös osztói, tehát e közös osztók legnagyobbika megegyezik. □

Köv.: Ha a és b egészek, akkor $(a, b) = (a - b, b) = (a - 2b, b) = \ldots = (a - kb, b)$. □

Két szám legnagyobb közös osztója hatékonyan meghatározható.

Euklideszi algoritmus: Input: a, b egészek (mondjuk $b \leq a$). Output: (a, b).

Legyen $a_0 := a$, $a_1 := b$. Ha már meghatároztuk az $a_0 \geq a_1 > \ldots > a_i$ számokat, akkor legyen $a_{i-1} = q_i a_i + a_{i+1}$, azaz osszuk el maradékosan a_{i-1}-t a_i-vel és legyen a_{i+1} a maradék, amire tehát $0 \leq a_{i+1} < a_i$ teljesül. Az eljárás akkor ér véget, ha $a_{k+1} = 0$. Ekkor az algoritmus válasza $(a, b) = a_k$.

Az euklideszi algoritmus helyességének igazolása: Az euklideszi algoritmus azért ér véget, azaz előbb-utóbb $a_{k+1} = 0$ lesz, mert (a_i) nemnegatív egészek csökkenő sorozata, tehát az eljárás lépésszámára $|a_0|$ felső becslés. Mivel $a_{i-1} - q_i a_i = a_{i+1}$, ezért az előző következmény miatt $(a, b) = (a_0, a_1) = (a_0 - q_1 a_1, a_1) = (a_2, a_1) = (a_1, a_2) = (a_1 - q_2 a_2, a_2) = (a_2, a_3) = \ldots = (a_k, a_{k+1}) = (a_k, 0) = a_k$. □

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

Az Euklideszi algoritmus segítségével egy másik fontos állítást is igazolunk.

Tétel: Tetszőleges $a \geq b$ egész számokhoz léteznek k és l egészek, melyekre $(a, b) = k \cdot a + l \cdot b$. Szavakban: bármely két egész legnagyobb közös osztója előáll a két egész szám *egészkombinációjaként*.[3]

Biz.: Hajtsuk végre az Euklideszi algoritmust az a és b számokra. Világos, hogy az $a_0 = 1 \cdot a + 0 \cdot b$ és az $a_1 = 0 \cdot a + 1 \cdot b$ számok előállnak az a és a b egészkombinációjaként. A teljes indukcióhoz tegyük fel, hogy az $a_0, a_1, \ldots, a_i$ számokra már bebizonyítottuk ugyanezt.

Az Euklideszi algoritmus definíciója alapján $a_{i-1} = q_i a_i + a_{i+1}$. Mivel a_i az a és b egészkombinációja, ezért $q_i a_i$ is előáll az a és b egészkombinációjaként. Nyilvánvaló, hogy egészkombinációk különbsége egészkombináció így $a_{i+1} = a_{i-1} - q_i a_i$ is az a és b egészkombinációja lesz. Ezek szerint $a_k = (a, b)$ is előáll az a és b egészkombinációjaként. □

Végül a prímszámokról közlünk néhány hasznos ismeretet.

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: Tetszőlegesen hosszú sorozat képezhető szomszédos összetett számokból, 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 $N + 1, N + 2, \ldots, N + n$ számok mindegyike összetett. □

A prímek eloszlásáról szólnak a következő állítások.

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

Dirichlet tétel: Ha a és d relatív prím, akkor az $a, a + d, a + 2d, \ldots$ számtani sorban végtelen sok prím fordul elő. □

Goldbach sejtés: Minden 2-nél nagyobb páros szám előáll két prím összegeként.

A Goldbach sejtésből azonnal következik a Csebisev tétel: ha $2n + 2$ mondjuk $p + q$ alakban áll elő, akkor p és q közül a nagyobbik $n + 1$ és $2n$ közé esik.

Nagy 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. □

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

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

Történelem Az első elemi bizonyítást a Csebisev tételre Erdős Pál találta még középiskolás korában.

A prímszámtétel bizonyítása több lépésben történt. Az utolsó lépést egymástól függetlenül Hadamard és de la Vallée Poussin tették meg 1896-ban. 1949-ben szintén furcsa holtverseny alakult ki az első elemi (felsőbb analízist nem használó) bizonyítások tekintetében: a befutók Atle Selberg és Erdős Pál voltak, akik egymás eredményeire támaszkodtak a bizonyításaikban. A két szerző között az eredmény Erdős általi bejelentését követően csúf vita támadt. Selberg a bizonyításért Fields érmet kapott, Erdős a kevésbé tekintélyes Cole díjat vehette át. Érdekesség, hogy a Selberg által bevezetett módszerrel később Chen igazolta a Goldbach sejtéssel kapcsolatos egyik legjobb ismert eredményt, mely szerint minden pozitív, páros szám előáll egy prím és egy olyan szám összegeként, amelynek legfeljebb két prímosztója van.

2.2 Kongruenciák, lineáris kongruenciák megoldása

Sokszor bizonyul hasznosnak az a megfigyelés, hogy egész számok összegének paritása csak az összeg tagjainak paritásától függ. (Pl egy összeg csak úgy lehet páratlan, ha páratlan számú (legalább egy) páratlan tagja van.) Azonban nem csak a kettővel való oszthatóságból származhatnak érdekes eredmények, hanem szükség lehet időnként arra, hogy más osztó szerint próbáljuk osztályozni az egészeket, és a szerint számoljunk velük. Ezt a gondolatot formalizáljuk az alábbiakban.

[3] Itt az egészkombináció kifejezés a lineáris kombinációra rímel. Arról van ugyanis szó, hogy míg lineáris kombinációban tetszőleges skalárok lehetnek az összeg tagjainak együtthatói, itt most csak egészek lehetnek az együtthatók.

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

Példa: $2 \equiv 17(5)$. A 2-vel kongruens számok modulo 5 a $2, 7, 12, 17, 22, \ldots$ ill. $-3, -8, -13, -18, \ldots$

Tetszőleges $m \geq 2$ egész esetén az egész számok $\mathbb{Z}$ halmaza m diszjunkt osztály uniójára bomlik fel, mégpedig úgy, hogy $0 \leq i \leq m-1$ esetén az i-dik osztályban az $k \cdot m + i$ alakú számok vannak, ahol k végigfut az egészeken. (Más szóval, az i-dik osztályba az m-mel osztva i maradékot adó számok tartoznak.) Ezeket az osztályokat az m *szerinti* (vagy másképpen *modulo* m) *maradékosztályoknak* nevezzük. A maradékosztályok jelentősége az, hogy ha két szám azonos maradékosztályba esik (modulo m), akkor kongruensek egymással modulo m, ha pedig különböző maradékosztályból valók, akkor nem kongruensek.

Állítás: 1. Ha $a \equiv b(m)$ és $c \equiv d(m)$ akkor $a + c \equiv b + d(m)$ és $ac \equiv bd(m)$, azaz két kongruencia összeadható és összeszorozható.
2.Ha $d \mid a$ és $d \mid b$ és $a \equiv b(m)$, akkor $\frac{a}{d} \equiv \frac{b}{d}(\frac{m}{(m,d)})$, azaz kongruencia osztásakor nemcsak a kongruencia két oldalát osztjuk, hanem a modulust is (az osztó és a modulus legnagyobb közös osztójával).

Biz.: 1. Tudjuk, hogy $m \mid a - b$ és $m \mid c - d$. Ezért $m \mid a - b + c - d = a + c - (b + d)$, azaz $a + c \equiv b + d(m)$. Az is igaz, hogy $m \mid c(a - b) + b(c - d) = ac - bd$, azaz $ac \equiv bd(m)$.

2. Legyen $a = a'd, b = b'd$, $D = (m, d)$, $d = d'D$ és $m = m'D$. Ekkor az $a \equiv b(m)$ kongruencia $a'd'D \equiv b'd'D(m'D)$ alakot ölt, ami definíció szerint azt jelenti, hogy $m'D \mid a'd'D - b'd'D = (a' - b')d'D$, azaz $m' \mid (a' - b')d'$ adódik. Mivel D az m és d legnagyobb közös osztója, ezért az $m' = \frac{m}{D}$ és a $d' = \frac{d}{D}$ számoknak már nem lehet közös prímosztójuk. Tehát $m' \mid a' - b'$ is igaz, ami éppen azt jelenti, hogy $a' \equiv b'(m')$, azaz $\frac{a}{d} \equiv \frac{b}{d}(\frac{m}{(m,d)})$. □

Sokszor az a célunk, hogy egy kongruencián ekvivalens átalakítást végezzünk, azaz ne csak a következtetésünk legyen helyes, hanem az utóbb kapott kongruenciából az eredeti is következzen. Erről szól az alábbi állítás.

Köv.: 1. Az $a \equiv b(m)$ kongruencia pontosan akkor teljesül, ha $a + k \equiv b + k(m)$.
2. Ha d relatív prím az m-hez, akkor az $a \equiv b(m)$ kongruencia ekvivalens a $ad \equiv bd(m)$ kongruenciával, tehát kongruencia szorzása csak akkor ekvivalens átalakítás, ha a modulushoz relatív prím számmal szorzunk.
3. Az $d > 0$ rögzített egész, akkor az $a \equiv b(m)$ kongruencia ekvivalens a $ad \equiv bd(md)$ kongruenciával.

Biz.: 1. Az, hogy az egyik kongruenciából következik a másik, a $k \equiv k(m)$ ill. a $-k \equiv -k(m)$ kongruencia hozzáadásával adódik.
2. Az $a \equiv b(m)$ kongruenciát a $d \equiv d(m)$ kongruenciával beszorozva $ad \equiv bd(m)$ adódik. Az osztásra vonatkozó állítás miatt pedig az $ad \equiv bd(m)$ kongruenciából $a \equiv b(\frac{m}{(m,d)})$ következik, ami $(m, d) = 1$ miatt $a \equiv b(m)$ alakot ölt.
3. $a \equiv b(m) \iff m \mid a - b \iff md \mid (a - b)d \iff md \mid ad - bd \iff ad \equiv bd(md)$. □

Tehát egy kongruencián ekvivalens átalakítás mindkét oldalhoz konstanst hozzáadni, a modulushoz relatív prímmel szorozni mindkét oldalt a modulus változatlanul hagyásával ill. az egész kongruenciát (a modulust is beleértve) egy számmal végigszorozni vagy leosztani. Rátérünk ezek után a lineáris kongruenciák tárgyalására.

Def.: *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 egy lineáris kongruenciával dolgozunk, akkor általában úgy végzünk műveleteket, hogy a kongruencia mindkét oldával ugyanazt tesszük. Az alábbi tétel segítségével könnyen elönthető, hány megoldása van egy adott lineáris kongruenciának.

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

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

Tegyük fel tehát, hogy $d \mid b$. A kongruenciát (a modulust is beleértve) d-vel végigosztva ekvivalens átalakításként végzünk, és azt kapjuk, hogy $a'x \equiv kb'(m')$, ahol $b' = \frac{b}{d}$. Mivel d az m és a legnagyobb közös osztója, ezért a leosztás után $(a', m') = 1$ áll. Az Euklideszi algoritmus után láttuk, hogy az Euklideszi algoritmus segítségével a lnko előáll egész kombinációként, azaz kiszámíthatunk olyan k és l egész számokat, amire $ka' + lm' = 1$. Világos, hogy k-nak és m'-nek nem lehet közös p prímosztója, hiszen ha volna, akkor $p \mid ka' + lm' = 1$ állna. Ezért k és m' relatív prímek.[4]

[4]Ez utóbbi megállapítás az előadáson nem hangzott el.

A $a'x \equiv b'(m')$ kongruenciának a modulushoz relatív prím k-val történő megszorzása ekvivalens átalakítás, azaz $ka'x \equiv kb'(m')$, ami k és l választása miatt $(1 - lm')x \equiv kb'(m')$ alakba írható. A kongruenciához hozzáadva az $lm'x \equiv 0(m')$ kongruenciát azt kapjuk, hogy $x \equiv kb'(m')$. Az elvégzett átalakítások ekvivalens volta miatt az $ax \equiv b$ kongruencia megoldásai pontosan azok az x egész számok, amik modulo m' a kb'-vel egy maradékosztályba tartoznak.

Hátra van még, hogy a megoldásokat modulo m adjuk meg. Minthogy $m = m'd$, ezért minden m' szerinti maradékosztály pontosan d darab m szerinti maradékosztály uniója, a konkrét esetben az alábbi reprezentánsokkal írható fel a megoldás: $x \equiv kb'(m)$, vagy $x \equiv kb' + m'(m)$, vagy $x \equiv kb + 2m'(m)$, vagy $\ldots$, vagy $x \equiv kb' + (d-1)m'(m)$. □

Megjegyzés: Az $a'x \equiv b'(m')$ kongruenciát az Euklideszi algoritmusból kapott k számmal történő beszorzással kaptuk meg. Ha nekünk nem lineáris kongruenciát, hanem az $ax = b$ lineáris egyenletet kellene megoldanunk, akkor a megoldás az a-val való osztás lenne, amit szerencsésebb úgy tekinteni, mint az a reciprokával történő szorzást. Az a reciproka a szokásos szorzás esetén természetesen $\frac{1}{a}$. A lineáris kongruencia fenti megoldásakor kapott k-val történő beszorzás teljesen hasonlóan működik, hiszen itt is azt kapjuk, hogy $ka' \equiv 1(m')$, tehát a szóbanforgó k tekinthető az a' reciprokának modulo m'. A fenti bizonyítás gondolatmenetéből az is adódik, hogy pontosan az m-hez relatív prím számoknak van modulo m reciproka.

Tehát, míg az $ax = b$ egyenlet pontosan akkor oldható meg, ha a-nak van reciproka vagy $a = 0$ és $b = 0$, addig lineáris kongruenciákra ez úgy módosul, hogy az $ax \equiv b(m)$ akkor megoldható, ha a-nak van „modulo m reciproka" vagy ha a-nak nincs (mert $(a, m) \neq 1$), akkor b-nek is „legalább annyira" nincs reciproka, azaz $(a, m) \mid (b, m)$.

Gyakran oldunk meg konkrét (mondjuk $ax \equiv b(m)$) lineáris kongruenciát ekvivalens átalakítások segítségével. Ennek során az alábbi átalakításokat végezzük.

1. Az a-t vagy a b-t vele kongruens másik számmal helyettesítjük.
2. Ha $(a, b) > 1$, akkor osztunk (szükség esetén az m modulust is)
3. A **modulushoz relatív prímmel** szorzunk (és a modulust nem bántjuk).

Az átalakítások során a cél az a együttható abszolút értékének csökkentése, egészen 1-ig.

Példa: Megoldandó a

$62x \equiv 24(36)$ kongruencia. Mivel $62 \equiv 26(36)$,ezért a
$26x \equiv 24(36)$ kongruenciát kapjuk. $(26, 36) = 2$, tehát osztunk:
$13x \equiv 12(18)$ adódik. Sajnos nem szorozhatunk $2, 3$ ill. 4-gyel, így inkább $13 \equiv -5(18)$-t helyettesítünk:
$-5x \equiv 12(18)$, majd szorzunk (-1)-gyel, mert nem szeretjük a negatív együtthatót.
$5x \equiv -12(18)$, ismét helyettesítünk:
$5x \equiv 6(18)$ Most jó lenne 4-gyel szorozni, hogy 2 legyen az együttható,
de ezt nem tehetjük, hisz a 2 nem relatív prím 18-hoz.
Viszont ügyesen észrevesszük, hogy 7-tel szorozhatunk:
$35x \equiv 42(18)$, és megint helyettesítünk:
$-x \equiv 6(18)$, szorzunk (-1)-gyel:
$x \equiv -6 \equiv 12(18)$. Most már csak a 36 modulusra kell áttérni:
$\underline{\underline{x \equiv 12(36)}}$ vagy $\underline{\underline{x \equiv 12 + 18 = 30(36)}}$, győztünk.

2.3 Redukált maradékrendszer, Euler-Fermat tétel

Most, hogy meg tudunk oldani lineáris kongruenciát, olyan hasznos tételeket mutatunk be, amik a modulo m számítások során lesznek segítségünkre. Az első szerint egy maradékosztály elemeinek a modulussal vett legnagyobb közös osztójuk megegyezik.

Megfigyelés: Ha $a \equiv b(m)$, akkor $(a, m) = (b, m)$. Speciálisan, ha egy maradékosztály valamely eleme relatív prím az m modulushoz, akkor annak a maradékosztálynak minden eleme relatív prím m-hez.

Biz.: Tudjuk, hogy $m \mid a - b$, ezért $b = a + km$ valamely k egészre. Az Euklideszi algoritmus előtt bizonyított tétel szerint viszont $(a, m) = (a + m, m) = (a + 2m, m) = \ldots = (a + km, m) = (b, m)$ □

Def.: Rögzített $m > 1$ egész esetén az m elemű $T = \{a_1, a_2, \ldots, a_m\}$ halmazt *modulo m teljes maradékrendszernek* nevezzük, ha T minden m szerinti maradékosztályból pontosan egy elemet tartalmaz. Az $R \subset \mathbb{Z}$ halmaz pedig *redukált maradékrendszer modulo m*, ha R minden olyan modulo m maradékosztályból, mely elemei relatív prímek m-hez pontosan egy elemet tartalmaz. A modulo m redukált maradékrendszer méretét, azaz azoknak az m szerinti maradékosztályoknak a számát, amik m-hez relatív prím számot tartalmaznak $\varphi(m)$-mel jelöljük.

Példa: Teljes maradékrendszer modulo m a $\{0, 1, 2, \ldots, m-1\}$ vagy az $\{1, 2, \ldots, m\}$ halmaz. Modulo 10 teljes maradékrendszer a $\{100, 21, -21, 42, -42, 13, -13, 44, 55, 66\}$ halmaz.

Megfigyelés: Redukált maradékrendszert pl. úgy kapunk , hogy egy teljes maradékrendszerből elhagyjuk a modulushoz nem relatív prím elemeket. Ezek szerint redukált maradékrendszert alkotnak az

1 és m közötti, m-hez relatív prím egészek. Ezért a $\varphi(m)$ függvényt definiálhattuk volna úgy is, mint az 1 és m közé eső, m-hez relatív prím számok számát. Ha p prím, akkor 1 és $p-1$ között minden egész relatív prím p-hez, ezért $\varphi(p) = p-1$.

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

Tétel: Legyen $(a,m) = 1$ és $k \in \mathbb{Z}$. Ha $R = \{r_1, r_2, \dots r_{\varphi(m)}\}$ redukált maradékrendszer modulo m és $T = \{t_1, t_2, \dots, t_m\}$ pedig teljes maradékrendszer modulo m, akkor $aR := \{ar_1, ar_2, \dots ar_{\varphi(m)}\}$ redukált maradékrendszer modulo m, $aT = \{at_1, at_2, \dots, at_m\}$ és $T + k = \{t_1 + k, t_2 + k, \dots, t_m + k\}$ pedig teljes maradékrendszerek modulo m.

Biz.: Azt kell igazolni, hogy az ar_i-k páronként különböző, m-hez relatív prím maradékosztályokhoz tartoznak, hisz ekkor szükségképpen minden relatív prím maradékosztályból pontosan egy reprezentáns szerepel. Minden ar_i relatív prím maradékosztályba tartozik, mert m-nek sem a-val, sem r_i-vel nincs közös prímosztója, így $(m, ar_i) = 1$. E maradékosztályok pedig különbözőek, hiszen ha $ar_i \equiv ar_j(m)$, akkor a-val oszthatunk az osztásról szóló következmény szerint, azaz $r_i \equiv r_j(m)$, ahonnan $i = j$ következik.

Az aT és $T + k$ halmazok teljes maradékredszer volta hasonlóan igazolható. Mindkét halmaz m elemű, ezért csak azt kell igazolni, hogy elemeik különböző m szerinti maradékosztályokba tartoznak. Ha pl $at_i \equiv at_j(m)$, akkor (a,m) miatt oszthatunk a-val, és $t_i \equiv t_j(m)$, amiből T TMR volta miatt $i = j$ következik. Hasonlóan, ha $t_i + k \equiv t_j + k(m)$, akkor $t_i \equiv t_j(m)$, azaz $i = j$. □

A fenti megfigyelésből 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 $R = \{r_1, r_2, \dots r_{\varphi(m)}\}$ redukált maradékrendszer modulo m. Az előző megfigyelés szerint $aR := \{ar_1, ar_2, \dots ar_{\varphi(m)}\}$ is redukált maradékrendszer modulo m. Mivel kongruenciákat lehet szorozni, ezért $\prod_i r_i \equiv \prod_i ar_i(m)$, ami azt jelenti, hogy $\prod_i r_i \equiv a^{\varphi(m)} \prod_i r_i(m)$. Mivel $(m, \prod_i r_i) = 1$, a modulus változtatása nélkül tuduk osztani, azaz $a^{\varphi(m)} \equiv 1(m)$, ami épp a bizonyítandó állítás. □

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 $(a,p) = 1$, 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 $a^p \equiv 0 \equiv a(p)$. □

Megjegyzés: Az Euler-Fermat tétel egyik jelentősége, hogy következik belőle a redukált maradékrendszerben a reciprok létezése, melyet a későbbiek miatt inverznek fogunk hívni. Ha tehát R egy redukált maradékrendszer modulo m, akkor azt mondjuk, hogy $r' \in R$ az $r \in R$ *inveze*, ha $rr' \equiv 1(m)$. Az Euler-Fermat tétel szerint tehát minden $r \in R$-nek létezik inverze, hiszen $r \cdot r^{\varphi(m)-1} = r^{\varphi(m)} \equiv 1(m)$, vagyis a $r' \equiv r^{\varphi(m)-1}(m)$ választás megfelelő. Világos, hogy ha r inverze r', akkor r' inverze r lesz. Az is könnyen adódik, hogy minden $r \in R$-nek pontosan egy inverze van: tegyük fel ugyanis, hogy $rr' \equiv 1(m)$ és $rr^* \equiv 1(m)$ valamely $r', r^* \in R$ esetén. Ekkor $rr' \equiv rr^*(m)$, és $(r,m) = 1$ miatt oszthatunk r-rel: $r' \equiv r^*(m)$, de ebből $r' = r^*$ következik. Érdemes még azt is látni, hogy az 1 és a -1 önmaguk inverzei.

Láttuk, hogy $\varphi(p) = p-1$, ha p prím. Ahhoz, hogy az Euler-Fermat tételt valóban használni tudjuk (pl. az inverz kiszámítására), jó ha ki tudjuk számítani $\varphi(m)$-t tetszőleges m modulusra. Prímhatvány-modulusra könnyű dolgunk van: ha $m = p^\alpha$ valamely p prímre, akkor a és m pontosan akkor relatív prímek , ha $p \nmid a$. Ezért $\varphi(m)$ nem más, mint 1 és m között a p-vel nem osztható egészek száma. A p-vel oszthatóak száma $\frac{m}{p} = p^{\alpha-1}$, így $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

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

Biz.: Azt kell meghatározni, hogy a $T = \{0, 1, 2, \dots, mn-1\}$ halmazban hány mn-hez relatív prím 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 T halmazban m-hez relatív prímek között hány szám relatív prím n-hez.

0	1	2	$\dots$	j	$\dots$	$m-2$	$m-1$
m	$m+1$		$\dots$	$m+j$	$\dots$	$2m-2$	$2m-1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
im	$im+1$	$im+2$	$\dots$	$im+j$	$\dots$		$(i+1)m-1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$(n-1)m$	$(n-1)m+1$		$\dots$	$(n-1)m+j$	$\dots$		$nm-1$

Írjuk fel a T halmaz elemeit növekvő sorrendben egy olyan táblázatba, melynek n sora és m oszlopa van. Ekkor az i-dik sor j-dik eleme $(i-1)m + j - 1$ lesz. Ha tehát rögzítünk egy oszlopot (vagyis egy j-t), akkor az ottani elemek azonos maradékosztályban lesznek modulo m. Mivel a táblázat m oszlopának mindegyike más-más mod m maradékosztálynak felel meg, ezért a táblázatban az m-hez relatív prím számok pontosan $\varphi(m)$ oszlopot töltenek ki. Vizsgáljunk egy oszlopot, azaz rögzítsünk egy j-t, és nézzük a j-dik oszlop meghatározta $\{j-1, m+j-1, 2m+j-1, \dots, (n-1)m+j-1\}$ halmazt.

Ezek a számok úgy keletkeznek, hogy az $T_n = \{0, 1, \ldots, n-1\}$ mod n teljes maradékrendszer minden elemét végigszorozzuk m-mel, majd hozzáadunk mindegyikükhöz $(j-1)$-et. Mivel $(n, m) = 1$, ezért minden oszlop egy teljes maradékrendszert alkot modulo n. Vagyis minden oszlopban pontosan $\varphi(n)$ db n-hez relatív prím elem található. Eszerint a táblázatban az olyan elemek, melyek m-hez is és n-hez is relatív prímek, $\varphi(m)$ oszlopban helyezkednek el, mindegyik oszlopban pontosan $\varphi(n)$ db. A keresett elemek száma tehát $\varphi(mn) = \varphi(m)\varphi(n)$. □

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

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

Biz.: A kanonikus alakban található prímosztók k száma szerinti teljes indukcióval bizonyítunk. A $k = 1$ esetet már láttuk. Egyébként $n = p_1^{\alpha_1} \prod_{i=2}^{k} p_i^{\alpha_i}$ és $(p_1^{\alpha_1}, \prod_{i=2}^{k} p_i^{\alpha_i}) = 1$, így az előző tétel szerint $\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(\prod_{i=2}^{k} p_i^{\alpha_i}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \prod_{i=2}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$. A második formula abból adódik, hogy $p^{\alpha} - p^{\alpha-1} = p^{\alpha}(1 - \frac{1}{p})$. □

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 $ab \equiv 1(p)$, hiszen az $ax \equiv 1(p)$ kongruenciát pontosan egy modulo p maradékosztály oldja meg. Könnyen látható, hogy ha a-hoz b tartozik, akkor b-hez a tartozik, tehát az $1, 2, \ldots, p-1$ számok úgy rendezhetőek párokba, hogy minden pár szorzata 1-et ad maradékul p-vel osztva.

A párokba rendezés azért nem egészen pontos, mert bizonyos számok esetleg önmagukkal állnak párban. Ezekre az a számokra $a^2 \equiv 1(p)$ teljesül, azaz $p \mid a^2 - 1 = (a+1)(a-1)$, ahonnan p prímtulajdonsága miatt $p \mid a+1$ vagy $p \mid a-1$ adódik. Eszerint az önmagukkal párban álló számok kizárólag a 1 és a $p-1$ lesznek.

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, és lesznek még a páratlanul maradt 1 illetve a $p-1$ tényezők. Más szóval $(p-1)! \equiv 1^{\frac{p-3}{2}} \cdot 1 \cdot (p-1) \equiv p-1 \equiv -1(p)$ adódik, és éppen ezt akartuk bizonyítani. □

A fenti gondolatmenetet felhasználva az az általánosabb tény is igazolható, hogy ha 1-től $(m-1)$-ig összeszorozzuk az m-hez relatív prím számokat, akkor a szorzat 1 vagy -1 maradékot ad m-mel osztva. Ha (a faktoriálisoknál maradva) azt szeretnénk tudni, milyen maradékot ad n-nel osztva az $(n-1)!$, 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 $(n-1)! \equiv 2(n)$.

3. fejezet

Általános algebra

3.1 Algebrai struktúrák, csoportok

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 félreértést okozni.

Példa: Kétváltozós művelet pl. a valós számokon az összeadás, szorzás, kivonás. A pozitív számokon az osztás és a hatványozás. Egyváltozós műveletnek tekinthető pl. az ellentett képzése (x-hez $-x$-t rendelünk), a pozitív számokon a reciprok vagy a 18 alapú logaritmus. Nullaváltozós művelet pl. az egészeken az, hogy 5. Háromváltozós művelet a valós számokon amely az x, y, z számokhoz $x(y + z) + \frac{\log|x^3|+5}{y^2+3}$-t rendel. A valós polinomokon kétváltozós művelet az összeadás, ill. a kompozíció (ami itt a behelyettesítés). Egyváltozós művelet a deriválás, vagy a $[0, x]$ intervallumon történő integrálás.

Nem művelet (ebben az 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.

Def.: Ha f_i egy, a H halmazon értelmezett n_i-változós művelet minden $i \in I$ esetén, akkor az $\mathcal{S} = \langle H, \{f_i : i \in I\}\rangle$ párt *algebrai struktúrának* mondjuk.

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.

A továbbiakban speciális algebrai struktúrákat fogunk tanulmányozni. A számunkra érdekes struktúrák kizárólag olyanok, melyeken a művelet kétváltozós. A félcsoportokon és csoportokon egy, míg a gyűrűkön és testeken két műveletet lesz értelmezve.

3.1.1 Félcsoportok és csoportok

Láttuk, hogy a műveletekre az egyetlen lényegi megkötés, hogy ne vezessenek ki az adott struktúrából, így aztán az ezekkel kapott algebrai struktúrák annyira általánosak, nem is várható, hogy jól használható, mély tételeket kapjunk. Célszerű tehát további megkötéseket tenni a vizsgált struktúrákra. Erre a legtermészetesebb mód, hogy a műveletektől 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 valós számokon értelmezett $+$ művelet asszociatív és kommutatív,
- a pozitív számokon értelmezett hatványozás nem asszociatív és nem kommutatív (hisz $2^{(2^3)} = 256 \neq 64 = (2^2)^3$ ill. $2^3 = 8 \neq 9 = 3^2$),
- a polinomok kompozíciója (egymásba helyettesítése) asszociatív, de nem kommutatív (hisz $[(p \circ q) \circ r](x) = p(q(r(x))) = [p \circ (q \circ r)](x)$ de $(p \circ q)(x) = p(q(x)) \neq q(p(x)) = (q \circ p)(x)$ általában),

- míg a valós számokon értelmezett *számtani közép* művelet kommutatív, de nem asszociatív (hisz $a \star b := \frac{a+b}{2} = \frac{b+a}{2} = b \star a$, de $(0 \star 0) \star 1 = 0,5 \neq 0,25 = 0 \star (0 \star 1)$).

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*.

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 van egységeleme, akkor egyetlen egységeleme van.

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: A $\langle \mathbb{R}, \{+, \cdot\} \rangle$ 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.

Megjegyzés: Ha a csoportműveletet $\cdot$ jelöli, és a csoport megadásakor ennek elhagyása nem okoz félreértést, akkor a fenti csoportot egyszerűen G-vel jelöljük. Ha nem okoz félreértést, akkor a $\cdot$ műveleti jelet a műveleteknél sem írjuk ki, így pl. a gh jelentése a g és h összeműveléseének (összeszorzásának) eredménye, azaz $g \cdot h$. A csoportban ezen konvenció értelmében beszélhetünk hatványozásról: egy g elem n-dik hatványa nem más, mint az elemet n-szer összeszorozzuk (egészen pontosan 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:

- $\langle \mathbb{R}, + \rangle, \langle \mathbb{Z}, + \rangle, \langle \mathbb{R} \setminus \{0\}, \cdot \rangle, \langle \mathbb{R}^{n \times k}$ (az $n \times k$ méretű valós mátrixok az (elemenkénti) összeadásra), $+ \rangle$ Abel csoportok.

- Ha $\mathbb{Z}_n$ jelöli a modulo n maradékosztályok halmazát, akkor $\mathbb{Z}_n$ a $+_n$-ra (modulo n összeadásra) csoportot alkot. Az egységelem a 0 maradékosztály.

- A $\mathbb{Z}_n$ halmazon a modulo n szorzás is egy asszociatív művelet, ráádásul az 1 maradékosztály egységelem erre a műveletre. De pl. a 0 maradékosztálynak nincs iverze, így a $\langle \mathbb{Z}_n, \cdot_n \rangle$ nem csoport, csak egységelemes félcsoport. Ha azonban $\mathbb{Z}_n^*$ jelöli az n-hez prím maradékosztályok halmazát, akkor belátható, hogy $\mathbb{Z}_n^*$ zárt a szorzásra, és ebben a struktúrában nemcsak egységelem van, de minden elemnek inverze is: az a maradékosztályának inverze az Euler-Fermat tétel miatt az $a^{\varphi(n)-1}$ maradékosztálya lesz. A $\langle Z_n^*, \cdot_n \rangle$ tehát (Abel) csoport.

- Nim összeadás, csienszüdzü (remélem, erre is lesz időm)

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

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

Példa: Láttuk, hogy $\mathbb{R}$ Abel csoport az összeadásra, és könnyen látható, hogy a pozitív valósak Abel csoportot alkotnak a szorzásra nézve. (Utóbbi esetben egységelem az 1, inverz a reciprok.) Érdemes azt is látni, hogy ez a két csoport lényegében ugyanaz: a (mondjuk 2 alapú) log függvény olyan bijekciót létesít a pozitív és a valós számok között, ahol a szorzásból összeadás lesz: $\log(a \cdot b) = \log(a) + \log(b)$. Csoportoknak az ilyesfajta azonosságáról szól az alábbi definíció.

Def.: (1) Két csoport (mondjuk G és H) *izomorf*, ha van köztük művelettartó bijekció, azaz létezik egy $\phi : G \to H$ bijekció, melyre tetszőleges $g, g' \in G$ esetén $\phi(g \cdot g') = \phi(g) \cdot \phi(g')$ áll. (Figyeljük meg, hogy a baloldali szorzás a G, a jobboldali pedig a H művelete.)
(2) A G csoport H részhalmaza a G *részcsoport*ja (jelölése $H \leq G$), ha H maga is csoport a G csoportműveletére.

Megfigyelés: Tetszőleges G csoport részcsoportjainak metszete is G részcsoportja.

Def.: Tetszőleges $K \subseteq G$ által *generált* $\langle K \rangle$ *csoport* a G csoport K-t tartalmazó részcsoportjainak metszete.

Megfigyelés: Ha G csoport, akkor tetszőleges $K \subset G$ esetén $\langle K \rangle$ a G csoport egy részcsoportja.

3.1.2 Ciklikus csoportok

Def.: Az olyan csoportot, melyet valamely eleme generál, *ciklikus csoport*nak nevezzük.
A G csoport g elemének *rendje* a g által generált $\langle g \rangle$ 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 ilyen n, 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 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 által generált e, g^i, g^{-i} elemek részcsoportot alkotnak (e az egységelem), ezért g éppen ezt a részcsoportot generálja, így 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 az 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 $g^l \cdot ((g^k)^{-1})^a = g^{ak+r} \cdot g^{-ak} = g^{ak+r-ak} = g^r \in H$, ami ellentmond k választásának. Tehát H-t g^k csakugyan generálja, vagyis H valóban ciklikus. □

3.1.3 Diédercsoportok

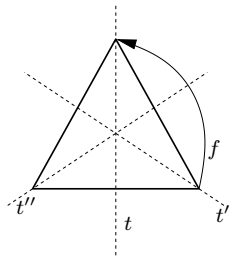
Fontos példák csoportokra a szimmetriák alkotta csoportok. Legyen X egy halmaz, és tekintsük $f : X \to X$ bijekcióknak egy olyan $\mathcal{F}$ nemüres halmazát, mely zárt a kompzícióra, vagyis $f, g \in \mathcal{F}$ esetén $f \circ g \in \mathcal{F}$, ahol $f \circ g(x) := f(g(x))$ $\forall x \in X$, továbbá, minden $f \in \mathcal{F}$ bijekció f^{-1} inverze is $\mathcal{F}$-ben van. A függvénykompozíció művelet definíció szerint asszociatív. A fenti választás éppen azt a célt szolgálta, hogy legyen egység és inverz, így e miatt $\langle \mathcal{F}, \circ \rangle$ 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 D_n csoport elemei az X egybevágóságai (azaz a sík mindazon egybevágóságai, melyek az X sokszöget (mint halmazt) fixen hagyják), a csoportművelet pedig az egybevágóságok egymás utáni elvégzése.[1] 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 D_n diédercsoportnak tehát $2n$ eleme van.

A $t \circ t = id$, $f^n = f \circ f \circ \ldots \circ f$[$n$-szer] $= id$ ill. $f \circ t = t \circ f^{n-1}$ 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. Lássuk a D_3 diédercsoport példáján, hogy néz ez ki a gyakorlatban!

[1] Van ám itt egy bosszantó konvenció. Nevezetesen, hogy az egybevágóságok voltaképpen függvények, márpedig egy függvény felírásakor az argumentumot a függvény jele *után* írjuk (zárójelek között): $f(x)$ módon. A függvénykompozíció definíciója szerint az $f \circ g$ függvény egy x értékhez az $(f \circ g)(x) := f(g(x))$ értéket rendeli. Ott okoz ez zavart, hogy ha csak az $f \circ g$ kifejezést látjuk, azt gondolhatnánk, hogy *először* kell az f-t és csak *utána* a g függvényt alkalmazni. Láttuk, hogy ennek épp a fordítottja igaz. A lényeg tehát, hogy a $\circ$ kompozícióműveletnél jobbról balra haladva kell a függvényeket sorban kiértékelni, ha minket a kompozíciófüggvény konkrét jelentése érdekel. Számolni a kompozícióval, mint művelettel azonban hajszálpontosan úgy kell, mint bármely más művelettel.

A szabályos háromszögnek t, t' és t'' jelöli a három szimmetriatengelyét, ill. f a középpontja körüli $\frac{2\pi}{3}$ szögű forgatást (az ábrán látható módon). Tudjuk, hogy $t^2 = id = f^3$, továbbá könnyen ellenőrizhető, hogy $f \circ t = t \circ f^2 = t'$, és ebből következően $f^2 \circ t = f \circ (f \circ t) = f \circ (t \circ f^2) = (f \circ t) \circ f^2 = (t \circ f^2) \circ f^2 = t \circ f^4 = t \circ f = t''$ áll. Tehát a D_3 diédercsoport hat egybevágósága az $id, f, f^2, t, t' = t \circ f^2$ és a $t'' = t \circ f$. Ezen összefüggések felhasználásával megkapható a D_3 csoport szorzótáblája is.



	id	f	f^2	t	$t' = t \circ f^2$	$t'' = t \circ f$
id	id	f	f^2	t	$t \circ f^2 = t'$	$t \circ f = t''$
f	f	f^2	id	$f \circ t = t'$	$f \circ t' = f \circ (t \circ f^2) = t''$	$f \circ t'' = f \circ (t \circ f) = t$
f^2	f^2	id	f	$f^2 \circ t = t''$	$f^2 \circ t' = f^2 \circ (t \circ f^2) = t$	$f^2 \circ t'' = f^2 \circ (t \circ f) = t'$
t	t	$t \circ f = t''$	$t \circ f^2 = t'$	$t \circ t = id$	$t \circ t' = t \circ (t \circ f^2) = f^2$	$t \circ t'' = t \circ (t \circ f) = f$
t'	t'	$t' \circ f = (t \circ f^2) \circ f = t$	$t' \circ f^2 = t' \circ f^2 = (t \circ f^2) \circ f^2 = t''$	$t' \circ t = (t \circ f^2) \circ t = f$	$t' \circ t' = id$	$t' \circ t'' = (t \circ f^2) \circ (t \circ f) = f^2$
t''	t''	$t'' \circ f = (t \circ f) \circ f = t'$	$t'' \circ f^2 = (t \circ f) \circ f^2 = t$	$t'' \circ t = (t \circ f) \circ t = f^2$	$t'' \circ t' = (t \circ f) \circ (t \circ f^2) = f$	$t'' \circ t'' = id$

Érdemes megfigyelni, hogy a forgatások (f hatványai) a D_n egy ciklikus részcsoportját alkotják.

3.1.4 Permutációcsoportok

Korábban már vizsgáltuk n elem lehetséges permutációinak számát; most a permutációk csoportstruktúráját vesszük szemügyre. Világos, hogy az $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ bijekciók zártak a kompozícióra és az inverzképzésre, ezért az $\{1, 2, \ldots, n\}$ halmaz permutációi szimmetriacsoportot alkotnak a kompozícióra.

Def.: Az S_n *szimmetrikus csoport* $\{1, 2, \ldots, n\}$ halmaz permutációi alkotta csoport a függvénykompozíció műveletre nézve.

Példa: Érdemes megnézni, hogyan hat konkrétan a függvénykompozíció a permutációkon. Egy π permutációt úgy adunk meg, hogy 1-től n-ig minden i-re meghatározzuk (mondjuk egy táblázattal megadva) $\pi(i)$ értékét. Emlékeztetünk, hogy a $\pi \circ \sigma$ permutáció kiszámításakor először alkalmazzuk a σ permutációt, és aztán a π-t. Konkrétan, ha például

$$\pi = \begin{array}{|c|c|c|c|c|}\hline 1&2&3&4&5\\\hline 2&4&3&1&5\\\hline\end{array} \qquad \text{és} \qquad \sigma = \begin{array}{|c|c|c|c|c|}\hline 1&2&3&4&5\\\hline 3&2&1&5&4\\\hline\end{array} \qquad \text{akkor} \qquad \pi \circ \sigma = \begin{array}{|c|c|c|c|c|}\hline 1&2&3&4&5\\\hline 3&4&2&5&1\\\hline\end{array} \qquad \text{adódik.}$$

Annak igazolásához, hogy a permutációkon a kompozíció csakugyan csoportot határoz meg, csupán annyit kell látni, hogy a kompozíció, mint kétváltozós művelet asszociatív (ez világos), létezik egységelem (az identikus (mindent helybenhagyó) leképezés egy permutáció, és ezzel akár jobbról, akár balról komponálunk, egységként viselkedik), ill., hogy minden π permutációnak létezik egy π^{-1} inverze, amire $\pi \circ \pi^{-1} = \pi^{-1} \circ \pi = id$, de az inverzleképezés (ami szintén permutáció) látnivalóan rendelkezik ezzel a tulajdonsággal.

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 $\{1, 2, \ldots, n\}$ 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.

Következő célunk a permutációk hatványait megvizsgálni, hogy konkrét permutációk rendjét meghatározhassuk. Legyen $i \in \{1, 2, \ldots, n\}$, $\sigma \in S_n$, 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 fenti példában szereplő permutációk felírása $\pi = (124)$ ill. $\sigma = (13)(45)$ lenne. *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 fix pontjain kívül 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 $(i_1, i_2, \dots, i_k)$ ciklikus permutáció a $(i_1, i_k), (i_1, i_{k-1}), \dots, (i_1, i_2)$ transzpozíciók szorzata, ezért az állítást igazoltuk. □

Értelmes kérdés, hogy legalább hány transzpozíció kell S_n generálásához. Minden transzpozíciónak megfelel egy él az $\{1, 2, \dots, n\}$ 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) hat. Tehát minden, transzpozíciókból álló generátorrendszernek összefüggő gráf felel meg, vagyis legalább $n-1$ transzpozíció kell S_n generálásához. Ennyi egyébként elegendő is: az $(1,2), (1,3), \dots, (1,n)$ transzpozíciók alkalmas kompozíciójával tetszőleges S_n-beli permutáció előállítható. Ennek belátásához elegendő azt megmutatni, hogy a fenti $n-1$ transzpozíció segítségével minden más transzpozíció előáll, hisz azok már –mint láttuk– minden permutációt generálnak. Konkrétan az (i, j) transzpozíció egy lehetséges előállítása $(i, j) = (1, j) \circ (1, i) \circ (1, j)$.

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 izomorf egy alkalmas permutációcsoporttal.

Biz.: Az általánosság megszorítása nélkül feltehető, hogy G n-edrendű, és G elemei az $1, 2, \dots, n$ számok. Ekkor G minden g elemének megfeleltethető egy σ_g permutáció az alábbiak szerint: $\sigma_g(i) := g \cdot i$. Ellenőrizzük, hogy a megfeleltetés műveletartó: $\sigma_{gh} = \sigma_g \circ \sigma_h$. Csakugyan, tetszőleges $i \in \{1, 2, \dots, n\}$ 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. □

3.1.5 A csoportelmélet alapjai

Ebben a részben véges csoportokkal foglalkozunk.

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.

Példa: Tetszőleges $n > 1$ pozitív egész esetén $H = \langle n\mathbb{Z}, + \rangle \leq \langle \mathbb{Z}, + \rangle = G$, ahol $n\mathbb{Z} := \{nz : z \in \mathbb{Z}\}$ az n többszöröseit jelöli. Egy adott $k \in Z$ esetén a G csoport k szerinti baloldali mellékosztálya a $k + nZ$ halmaz lesz, vagyis mindazon egészek, melyek k-val kongruensek modulo n.

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 (g által generált részcsoport elemszáma) osztja G rendjét.

Biz.: Az előző megfigyelés szerint a G csoport néhány H szerinti (jobboldali) mellékosztály uniója, és minden mellékosztály $|H|$ elemet tartalmaz. □

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

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

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. □

3.2 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 a szorzást is) 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. $(a+b)c=ac+bc$ $(\forall a,b,c\in R)$. 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 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 $\langle R,+\rangle$ részcsoportja a $\langle\mathbb{Z},+\rangle$ csoportnak. Mivel az utóbbi csoport ciklikus, ezért minden részcsoportja is az, tehát R-t egyetlen elem (mondjuk az n) generálja, ezért $R=n\mathbb{Z}$. □

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 ellentettjével szorozni, hiszen a szorzás nem csoport- (csak félcsoport-) 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 invertálhatóságának nem kell ennél jobban sérülnie.

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. (Láttuk, hogy kommutatív gyűrű. Minden nemnulla számnak van reciproka, így a szorzás is csoport a nemnulla számokon.)
(2) Ha p prím, akkor $\mathbb{Z}_p$ test, melynek a szokásos jelölése $\mathbb{F}_p$. (Láttuk, hogy $\mathbb{Z}_p$ kommutatív gyűrű, és az Euler-Fermat tételből adódik a reciprok kiszámítása.) Ha m nem prím, akkor (láttuk) van $\mathbb{Z}_m$-ben nullosztó, 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 (azaz a valós polinomok gyűrűjét) 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 $(a+b\sqrt{2})^{-1}=\frac{1}{(a+b\sqrt{2})}=\frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\frac{a}{a^2-2b^2}+\frac{-b}{a^2-2b^2}\sqrt{2}$ miatt létezik inverz. (Itt használtuk, hogy ha $a,b\in\mathbb{Q}$, akkor $a^2\neq 2b^2$. Igaz az is, hogy a példabeli $\sqrt{2}$ helyett állhatna $\sqrt{t}$ is $(0<t\in\mathbb{Q}_+)$.

4. fejezet

Számítási algoritmusok, kriptográfia

4.1 Algoritmusok bonyolultsága

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 feltett 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. Ez a függvény minden n-re meghatározza azt az $f(n)$-t, ami az algoritmus legnagyobb lépésszáma egy n hosszú bemenet esetén. (Feltételezzük, hogy az algoritmus minden bemeneten előbb-utóbb megáll.) Ha egy A ill. A' algoritmus f ill. f' lépésszámfüggvényeire minden n esetén $f(n) \leq f'(n)$ áll, akkor bizonyos értelemben[1] jogos az A algoritmust hatékonyabbnak tekinteni, mint az A' algoritmust. Mi van azonban akkor, ha bizonyos n-ekre $f(n) \leq f'(n)$, 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 $10^5 \cdot n$, az A'-é 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 algoritmus 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. Paradox módon jobbnak tekintünk tehát egy $10^{10^{10}} \cdot n^{10^{10}}$ lépésszámú algoritmust, mint egy $(1 + 1/10^{10^{10}})^{n/10^{10^{10}}}$ futásidejűt, még akkor is, ha a gyakorlatban az előbbi már $n = 2$ méretű bemenet esetén is kivitelezhetetlen, míg az utóbbi akkor is működik, ha a bemenet mérete a hihetetlenül hatalmas számok világából való. Még egyszer tehát az Állatfarmba 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.) Egy algoritmust a továbbiakban *polinomiálisnak* (néha, kissé félreérthetően *hatékonynak*) nevezünk, ha lépésszáma (így közvetve a futásideje) a bemenet méretének polinomjával felülről becsülhető.

[1] Tehát rosszabb egy A algoritmus, ami az inputok 99,99%-án szinte azonnal végez, de néhány szerencsétlen inputon „elszáll", mint az az A' algoritmus ami minden inputon sokat erőlködik, de azért mindig megbízhatóan végez. Ez pl. akkor lehet különösen indokolt, ha az a fontos, hogy belátható időn belül megoldjuk a problémát (pl., hogy kiszámítsuk az űrhajó pályamódosítását, a szembejövő meteor miatt, vagy atomerőművet vezéreljünk), mert az időtúllépések nem „átlagolódnak ki": egyetlen szerencsétlen input, és game over.

4.1.1 Néhány egyszerű eljárás bonyolultsága

Megvizsgálunk néhány, számokkal operáló algoritmust hatékonyság szempontjából. Az algoritmus bemenete tehát néhány (általában két) szám, ezekkel végzünk műveletet. 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: Az n^m szám jegyeinek száma kb $k \cdot 2^l$, ahol k és l az n ill. m jegyeinek száma 2-es számrendszerben. Mivel itt a bemenet mérete $k+l$, ezért a végeredményt még leírni sem tudjuk a bemenet hosszának polinomjával becsülhető lépésben. Így, mivel már az eredmény megadása is exponenciálisan sok időt igényel, nem létezik a hatványozásra polinomiális algoritmus.

Hatványozás modulo m: Az input n, k és m, a cél pedig $n^k (\mathrm{mod}\ m)$ meghatározása.

Legyen $k = \sum_i k_i 2^i$, azaz $k = \underline{\ldots k_2 k_1 k_0}_2$ 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. A szükséges n_i-k kiszámításához mindezt $\log k$-szor kell megtenni. Az n^k meghatározását pedig $n^k = \prod_{i=1}^{\infty} n^{k_i 2^i} \equiv \prod_{i=1}^{\infty} n_i^{k_i}(m)$ alapján további, legfeljebb $\log k$ db, legfeljebb $\log m$ méretű szám szorzásával és $\log k$ db, legfeljebb $2 \log m$ méretű szám maradékos osztásával kapjuk.

Példa: Ha pl az $n^{23} (\mathrm{mod}\ m)$-t szeretnénk kiszámítani, akkor kiszámítjuk an $n (\mathrm{mod}\ m)$, $n^2 (\mathrm{mod}\ m)$, $n^4 \equiv (n^2)^2 (\mathrm{mod}\ m)$, $n^8 \equiv= (n^4)^2 (\mathrm{mod}\ m)$, és $n^{16} \equiv (n^8)^2 (\mathrm{mod}\ m)$ értékeket modulo m, ami négy szorzással (ahol a tényezők m-nél nem nagyobbak) és öt (m-mel való) maradékos osztással jár. Ezután $n^{23} \equiv n^{16} \cdot n^4 \cdot n^2 \cdot n (\mathrm{mod}\ m)$ miatt további három szorzás (a tényezők m-nél nem nagyobbak) és három maradékos osztás szolgáltatja a végeredményt.

A modulo m hatványozás tehát összességében is polinomiális eljárás.

Euklideszi algoritmus: Az euklideszi algoritmus egy lépésében adott $a_{i+1} \leq a_i$ esetén kell egy maradékos osztást végezni, és meghatározni azt a $0 \leq a_{i+2} < a_{i+1}$-t, melyre $a_i = q_{i+1} \cdot a_{i+1} + a_{i+2}$ áll. Az a_i mérete legfeljebb akkora, mint a_0 és a_1 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 $\log a_0$-szor kell elvégezni, amitől az eljárás polinomiális marad.

4.2 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 (lépésszáma n-ben lineáris, ami $\log n$-ben exponenciális), sem a naív módszer (ebben 1-től $\sqrt{n}$-ig ellenőrizzük az oszthatóságot $\sqrt{n}$-ben lineáris számú osztással).

A prímtesztelés kemény dió. Létezik ugyan rá olyan determinisztikus algoritmus, ami egyúttal polinomiális is, de ilyet csak a legutóbbi időben találtak. Ehelyett mutatunk egy sokkal gyakorlatibb módszert, aminek az a hibája, hogy nem ad halálbiztos eredményt. Megengedjük ugyanis a véletlen választást is az algoritmus futása során, amiből az következik, hogy az eljárás nem lesz tévedhetetlen. A módszer azonban csak egy irányban 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 n összetettségéről meggyőződni, hogy találunk egy olyan $0 < k < n$ számot, amire $(k,n) \neq 1$. Ekkor az euklideszi algoritmus az n egy valódi osztóját is megtalálja, ezért k még további információt ad n-ről. Az ilyen k számok az n *leleplezői*. Akárcsak a árulókra, a leleplezőkre is igaz hogy $k^{n-1} \not\equiv 1 \pmod{n}$, hiszen k^{n-1} nem relatív prím n-hez ha k sem volt az, tehát nem lehet a redukált maradékrendszer eleme sem.

Persze az is megtörténhet, hogy n összetett, és 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.[2]

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 valók. 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. □

A prímtesztelésre egy lehetséges módszer tehát a következő. Véletlenül választunk egy $0 < k < n$ számot. Ha k árulója vagy leleplezője n-nek, azaz $k^{n-1} \not\equiv 1 \pmod{n}$, 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 $k^{n-1} \not\equiv 1(n)$ **then STOP:** n nem prím.

else STOP: úgy tűnik, n prím

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 legfeljebb $\frac{1}{2^m}$ 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 n-nek létezik árulója. Vannak azonban olyan számok (az ú.n. *álprímek*, vagy más néven *Carmichael számok*), amiknek csak cinkosai és leleplezői vannak (utóbbiak elenyésző számban). Az ismételt Fermat-teszt ezeket a számokat majdnem biztosan prímnek találja. Olyan módszert szeretnénk tehát, ami a mégoly ritka álprímekre is teljesen megbízhatóan működik. A Fermat-teszt a fő lépésében azt ellenőrzi, vajon teljesül-e, hogy $n \mid k^{n-1} - 1$. Ha ugyanis n prím, akkor ez minden $0 < k < n$-re teljesül. Ennél azonban több is igaz. Ha t.i. $n - 1 = 2^t \cdot q$, ahol q páratlan, akkor az $(x+y)(x-y) = x^2 - y^2$ azonosság többszöri alkalmazásából az adódik, hogy

$$k^{n-1} - 1 = k^{2^t q} - 1 = (k^{2^{t-1} q} - 1)(k^{2^{t-1} q} + 1) = (k^{2^{t-2} q} - 1)(k^{2^{t-2} q} + 1)(k^{2^{t-1} q} + 1) = \ldots =$$
$$= (k^q - 1) \cdot (k^q + 1)(k^{2q} + 1)(k^{4q} + 1) \cdots (k^{2^{t-1} q} + 1) \; . \tag{4.1}$$

Tehát ha $n = p$ prím, akkor p a (4.1) jobboldalának valamelyik tényezőjét is osztja. Hiába osztható tehát a baloldal n-nel: ha a jobboldal egyetlen tényezője sem n többszöröse, akkor n bizonyosan összetett, és k az n szám egy *Carmichel értelemben vett árulója*[3]. Igaz, hogy minden összetett szám redukált maradékrendszerének legalább $\frac{3}{4}$-edrésze Carmichael értelemben vett áruló. Ezért a (4.1) 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.

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 összetett szám van 1 és $2,5 \cdot 10^{10}$ között, aminek $k = 2, 3, 5, 7$ mindegyike Carmichael-cinkosa. Az összes többi összetett szám kiszűrhető négy Miller-Rabin teszt elvégzésével a fenti k értékekre.

[2] 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 szükséges fogalmakat a csoportelmélet résznél tárgyaljuk.

[3] Figyeljük meg, hogy ha k cinkos, de Carmichael értelemben vett áruló, akkor az (4.1) jobboldalán álló tényezők valamelyike leleplező, így az Euklideszi algoritmussal megtalálható n egy osztója is.

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

4.3 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 $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ függvényt, ha f bijekció, mely hatékonyan (azaz polinomiális időben, és a gyakorlatban is gyorsan) számítható, azonban a fordított irányú f^{-1} leképezés kiszámítása pusztán f ismeretében reménytelen. (Pl. ha megvan a telefonkönyv, akkor egy adott személyhez hamar 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} is 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 biztonsága a kiskapus egyirányú függvények létezésére épít, nem tudjuk teljes bizonyossággal, vajon csakugyan léteznek-e kiskapus egyirányú függvények. Vannak azonban függvények, melyekről azt *sejtjük*, hogy ilyenek, de bebizonyítani ezt nem tudjuk. (Így aztán mindig van min dolgozniuk a rejtjelfejtő szakembereknek.)

Egy titkosírási rendszernél rögzítünk egy Σ-val jelölt 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. Feltehetjük, hogy Σ^t szavai 1 és $|\Sigma|^t$ közötti természetes számoknak felelnek meg (pl. $\Sigma = \{0, 1\}$ esetén a bináris alak egy ilyen megfeleltetés, egyébként az üzenetet egy $|\Sigma|$ alapú számrendszerben felírt számnak tekintjük). A nyilvános kulcsú titkosírási rendszert egy olyan kiskapus egyirányú $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ függvény írja le, melyre $n \geq |\Sigma^t|$. Ezt a leképezést egy ú.n. *nyilvános kulcs* segítségével egyértelműen megadjuk, és bárki számára hozzáférhetővé tesszük. Feltételezzük továbbá, hogy az A-nak nevezett címzett, akinek a titkosított információt 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, amit a nyilvános kulcs ismeretében könnyen megtehetünk. Ezután M'-t 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. A lehallgató mindössze arra képes, hogy ha valamilyen égi sugallat folytán megsejti, mi is az üzenet, akkor ellenőrizni tudja, csakugyan azt küldték-e el. Nem árt azért picit óvatosnak lenni. Ha például a lehallgató tudja, hogy az üzenet 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.)

A nyilvános kulcsú titkosírás alkalmas a *digitális aláírás* megvalósítására is, azaz segítségével bizonyítható, hogy egy adott üzenet kitől érkezett. Nevezetesen, tegyük fel, hogy minden szereplőnek van egy kiskapus egyirányú függvénye, pl. A-é f_A, míg B-é f_B. Ha most B alá akarja írni az M (titkosított vagy titkosítatlan) üzenetet, akkor A-nak az $M' = f_B^{-1}(M)$-t küldi el. Ezt A vissza tudja fejteni a nyilvános f_B leképezés ismeretében, hiszen $f_B(M') = f_B(f_B^{-1}(M)) = M$. Ráadásul a címzett bárki más (pl. a bíróság) számára is bizonyítani tudja, hogy az üzenetben egyfelől az áll, amit állít, másrészt, hogy az üzenet B-től ered. Ha ugyanis A felfedi M-t, és M'-t, akkor bárki ellenőrizheti B nyilvános kulcsának ismeretében, hogy $M = f_B(M')$, vagyis, hogy B valóban aláírta az M üzenetet. Ha pedig M egy A-nak

szánt titkos üzenet volt, azaz $M = f_A(M^*)$, ahol M^* az igazi üzenet, akkor f_A nyilvános volta miatt bárki láhatja, hogy M az M^* titkosított változata. Az előbbiek szerint bizonyítható, hogy az M kódolt üzenetet B aláírta, tehát a digitális aláírás titkosított üzenetek esetén is használható. Fontos, hogy a bizonyításhoz csak a nyilvános kulcsokra van szükség: egyik félnek sem szükséges felfednie a titkos kulcsát.

Nézzük meg, hogyan lehet a fenti sémát megvalósítani, azaz hogyan lehet egy kiskapus egyirányúnak sejtett függvényt megadni. Az alábbiakban a nyilvános kulcsú RSA[4] rendszert vázoljuk.

Ahhoz, hogy bárki is titkosított levelet tudjon küldeni az A címzettnek, A előzőleg választ két kellően nagy prímszámot, mondjuk p-t és q-t. A kellően nagy azt jelenti, hogy a tudomány aktuális állása szerint reménytelen legyen a $n := pq$ szorzat faktorizálása, továbbá $n \geq |\Sigma^t|$ is teljesüljön. (Ez utóbbi úgy teljesíthető, hogy az üzenetdarabok t hosszát alkalmasan választjuk.) Legyen $m := \varphi(n) = (p-1)(q-1)$ és válasszuk az $1 \leq e \leq n$ számot úgy, hogy $(e, m) = 1$ teljesüljön (ilyen e könnyen található[5]), és legyen $f(M) := M^e (\mathrm{mod}\ n)$. Ha ez megvan, akkor A közhírré teszi a nyilvános kulcsát, azaz mindenki számára hozzáférhetővé teszi az n és e számokat, hiszen ennek segítségével bárki hatékonyan tudja f-t számítani, azaz képes lesz A számára titkos üzenetet küldeni. Hangsúlyozzuk, hogy A titokban tartja a p, q és m számokat.

Természetesen A kíváncsi arra, mit tartalmaznak a neki címzett titkos üzenetek, ezért szüksége van arra, hogy az f^{-1} leképezést hatékonyan tudja számítani. Ehhez először megoldja d-re az $ed \equiv 1(m)$ kongruenciát, amit $(e, m) = 1$ miatt egyértelműen (és hatékonyan) megtehet. Annak, aki nem ismeri m-t, ez a feladat –úgy hisszük– reménytelen, így azt feltételezzük, hogy A-n kívül senki sem képes n és e alapján d-t kiszámítani. (Látjuk persze, hogy ha az n-t valaki faktorizálja, akkor m-t majd d-t könnyűszerrel kiszámíthatja. A titkosírási rendszer megtöréséhez azonban még csak erre sincs szükség: elég, ha valahogyan megszerzi m-t, mert d már akkor is meghatározható. Ha tehát A bölcsen jár el, akkor nyomban azután, hogy d-t kiszámította, megsemmisíti minden addigi számítását, különös tekintettel a p, q és m számokra.)

A d meghatározásával A megkapta az (n, d) *titkos kulcsot*, amit élete árán is megőriz. Az inverzleképezés ugyanis pontosan úgy működik, mint a nyilvános kulcsú titkosítás, csak persze a nyilvános helyett a titkos kulccsal. Konkrétan: ha A egy $X = f(M)$ titkosított üzenetet kap, akkor a dekódolt üzenet $f^{-1}(X) = X^d \pmod{n}$. Valóban:

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

az Euler-Fermat tétel miatt. (A fenti számolásnál az $(X, n) = 1$ feltételezéssel éltünk. Belátható, hogy a fenti inverztulajdonság a mégoly valószínűtlen $p \mid X$ és $q \mid X$ esetekben is igaz.) Tehát az (n, d) titkos kulcs ismeretében az inverzleképezés is hatékonyan számítható, ahogyan ezt egy kiskapus egyirányú függvénytől elvárjuk. Azt is láttuk, hogy (n, 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 miképtje 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. A prímeket ráadásul úgy kell találni, hogy minden prímet lehetőleg egyforma eséllyel válasszunk, hisz ha bizonyos prímekhez túl nagy valószínűséggel nyúlunk, akkor ez könnyít a kódtörő helyzetén. Az első ötlet, hogy próba szerencse alapon keresünk prímet, azaz választunk egy (kellően nagy) véletlen számot: ha prím, győztünk, ha nem, újat húzunk. Ez a módszer valóban működik, ehhez persze szükség van egy hatékony prímtesztre (ilyet már láttunk), másrészt az is követelmény, hogy ne kelljen túl sok véletlen számot generálni, míg valahára egy prímnél kötünk ki. Szerencsére ez is teljesül: a prímszámtétel egy erősebb alakja szerint a prímek sűrűsége n közelében nagyon jó közelítéssel $\frac{1}{\ln n}$, azaz e^{461} (azaz a 200 jegyű számok) környékén véletlen számokat választva kb. $\frac{1}{500}$ valószínűséggel prímet találunk. Vagyis

[4] A név a rendszert kifejlesztő Rivest, Shamir és Adleman neveinek kezdőbetűiből származik. E három szerző mutatott rá először a digitális aláírás lehetőségére, és írt le először egy a mai napig kiskapus egyirányú függvénynek gondolt leképezést.

[5] Itt sem árt észnél lenni: ügyetlen választásnál a rendszer támadhatóvá válik. (Pl. az $e = 1$ egy matematikailag korrekt, ám hiperbuta választás.) Van arra vonatkozó általános irányelv, hogyan érdemes e-t választani ahhoz, hogy a rendszer biztonsága ettől ne sérüljön. (Vagy egy kicsit pesszimistábban fogalmazva: ne ettől sérüljön.) Természetesen, ahogy egyre újabb támadási módszereket eszelnek ki (és hoznak nyilvánosságra), úgy az „általános irányelv" is időnkénti módosításra szorul. Arany életük van az elméleti kriptológusoknak.

$500 \cdot k$ próbálkozás után kb e^{-k} a valószínűsége annak, hogy nem akadt prím a horogra[6].

Történelem: Ha sok időm lesz, erről is írok még...

[6] A próbálkozások várható száma jelentős mértékben csökken, ha kiszűrjük a kis prímekkel osztható (legegyszerűbb esetben a páros) számokat, azokat rögtön eldobjuk, és nem teszteljük.