Bevezetés a számításelméletbe II.

2014-es tételsor kidolgozva

Demeter Deli Kristóf 2014-es kidolgozott tételsora alapján
készítette Heilig Benedek

Tartalomjegyzék

Első tétel

Szélességi keresés haszálata az összefüggőség eldöntésére, Euler-séta és -körséta, létezésük szükséges és elégséges feltétele. Hamilton-körök és -utak. Szükséges feltétel Hamilton-kör/út létezésére. Elégséges feltételek: Dirac és Ore tétele.

Euler-körséta (-séta)

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

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

1. G-nek pontosan akkor van Euler-körsétája, ha G minden csácsa páros fokú, illetve
2. G-nek pontosan akkor van Euler-sétája, ha G-nek 0 vagy 2 db páratlan fokú csúcsa van.

Bizonyítás:

1. (a) *Szükségesség:* A séta éleit az áthaladás szerint irányítva minden csúcsba annyi él megy be, amennyi ki. A csúcs foka ezek összege, ami páros szám.

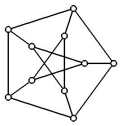
   (b) *Elégségesség:* G-re élszám szerinti indukcióval. 0 élű gráfban igaz. Tegyük fel hogy m élűnél kevesebb élű gráfokra már bizonyítottuk az állítást. Legyen G-nek m éle. Ekkor G-ben létezik egy C kör, mert minde foka páros, bárhonnan indulunk el (bármely csúcsból) biztosan visszajutunk oda. Hagyjuk el a C kört. Ekkor G olyan komponensekre esik szét, ahol minden csúcs foka páros ($\forall$ komponensből pontosan 2 élt hagytunk el). Így az indukciós feltevés alapján (<m élünk van) van bennük Euler-körséta. Ebből úgy kapjuk G Euler-körsétáját, ha a C kör mentén haladva minden komponensbe érkezéskor annak Euler-körsétáján haladunk tovább, majd ha azzal végeztünk folytatjuk az utat C mentén. Így megkapjuk G Euler-körsétáját.

2. Ha G $\forall$ foka páros, akkor 1. miatt létezik Euler-körsétája, emiatt Euler-sétája is. Ha 2 páratlan foka van, húzzunk be egy élet a kettő között, ekkor 1. miatt van Euler-körsétája. A behúzott élet utolsónak véve és elhagyva pedig G Euler-sétáját kapjuk. (Nem kell G-nek egyszerűnek lennie, párhuzamos éllel is működik.)

Hamilton-kör (-út)

Definíció: A G gráf Hamilton-köre (-útja) a G egy olyan köre (útja), mely G minden csúcsát tartalmazza. Mivel egy körben (útban) szereplő minden csúcs különböző, ezért a Hamilton-körben (-útban) is minden csúcs pontosan egyszer szerepel.

Tétel: Ha a véges G gráfban létezik Hamilton-kör (-út), akkor a G tetszőleges k pontját törölve a gráf legfeljebb k (k+1) komponensre esik szét. *Bizonyítás:* Ha G Hamilton-kör (-út) akkor világos, ha pedig további élei is vannak, akkor nem eshet szét több komponensre. Ez a feltétel szükséges a Hamilton-kör (-út) létezéséhez, de nem elégséges. Pl: a Petersen-gráfnak nincs Hamilton-köre, mégis teljesíti az állítást.



Elégséges tételek a Hamilton-kör létezésére (erősségi sorrendben visszafelé következnek egymásból)

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

Ore tétele: Ha az $n \geq 3$ pontú, egyszerű G gráf olyan, hogy bármely 2 nemszomszédos csúcs fokszámösszege legalább n, akkor G-nek létezik Hamilton-köre.

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

Ore tételének bizonyítása: Legyen G egy ellenpélda a tételre. Ekkor - mivel további élek behúzása nem rontja el az Ore-tulajdonságot - feltételezhetjük, hogy egy új él behúzása létrehoz egy Hamilton-kört, azaz G bármely két nemszomszédos csúcsa között vezet Hamilton-út. Így, ha u és v nem szomszédos csúcsok, akkor létezik egy P Hamilton-út u-ból v-be: $u = v_1, v_2, \ldots, v_n = v$. Ekkor ha v_k a gráf éle, akkor $v_{k-1}v_n$ nem lehet a gráf éle, mert $v_1, v_2, \ldots, v_{k-1}, v_n, v_{n-1}, \ldots, v_k, v_1$ a gráf egy Hamilton-köre lenne, pedig G-ben nincs Hamilton-kör. Ha így $v_1(= u)$ 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 közül egy sem, azaz a v_n szomszédainak száma legfeljebb $n - 1 - m$ lesz. Így $d(v_1) + d(v_2) \leq m + n - 1 - m = n - 1 < n$, ellentmondásra jutottunk, tehát a tétel igaz.

Szélességi keresés/bejárás (Breadth-first search)

1. Kiindulunk egy v_0 gyökérből, és bejárjuk v_0 bejáratlan szomszédait. Legyenek ezek $v_1, v_2, \ldots, v_k$.
2. Ha már nem tudjuk v_0 bejáratlan szomszédait bejárni, bejárjuk v_1 bejáratlan szomszédait $(v_{k+1}, v_{k+2}, \ldots, v_{k+l})$
3. Ezután v_2 bejáratlan szomszédait, majd a soron következőket az előbbiek alapján. A még bejáratlan pontokat mindig a sor végére tesszük.
4. Ha már nem tudunk több pontot bejárni, akkor választunk egy új gyökeret, és onnan folyatatjuk.

Ha nem tudtuk a gráfot egy gyökérből bejárni, akkor nem összefüggő.

Második tétel

Páros gráf fogalma, kapcsolat a páratlan körökkel. Párosítások a páros gráfban, a javítóutak módszere, Hall és Frobenius tételei.

Páros gráf

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

Ez azzal ekvivalens, hogy: a G gráf pontosan akkor páros, ha a csúcsai két diszjunkt halmazba oszthatóak úgy, hogy egy halmazon belül nem fut él.

Állítások:

1. Minden páros hosszú kör páros gráf. (Felváltva színezés)
2. Ha egy páros gráf páros, akkor minden részgráfja is páros.
3. Páros gráf nem tartalmazhat páratlan kört (Legalább 3 szín kell hozzá)

Tétel: A G véges gráf pontosan akkor páros, ha G nem tartalmaz páratlan kört.

Következmény: Minden fa páros gráf.

Bizonyítás:

1. *Szükségesség:* 3. állítás a színezés miatt.
2. *Elégségesség:* Tegyük fel, hogy G nem tartalmaz páratlan kört. Mivel élek csak komponensen belül futnak, feltehetjük hogy G összefüggő. Legyen F a G egy feszítőfája, és v a G egy testszőleges pontja, a fa gyökere. Legyen A a v-től az F fán páros távolságra lévő pontok halmaza, B a páratlanra lévőké. F minden éle A és B között fut (mert fa), de megmutatható, hogy ez G-re is igaz. Ha teljesül akkor 2-színezhető $\Rightarrow$ páros.
   Tegyük fel, hogy G egy éle xy az A halmazok (B-re ugyanígy) belül fut. Ekkor létezne G-ben páratlan husszú körséta: $xy \dots v \dots x$. Ebből elhagyva $xy \dots v$ és $v \dots x$ közös részét, amely kétszer szerepel a körsétában (páros hosszú) egy páratlan kört kapunk. Ez ellentmondás $\Rightarrow$ G páros.

Párosítás

Definíció: 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.

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

Frobenius tétele: A G véges, páros gráfnak pontosan akkor létezik teljes párosítása, ha $|A| = |B|$ és $|X| \leq |N(X)|$ minden $X \subseteq A$ ponthalmazra, ahol A és B a két diszjunkt csúcsosztály G-ben.

Hall tétele: A G véges, páros gráfnak pontosan akkor létezik A-t fedő párosítása, ha $|X| \leq |N(X)|$ minden $X \subseteq A$ ponthalmazra. A és B a két diszjunkt csúcsosztály G-ben.

Frobenius tételének bizonyítása:

1. *Egyik irány:* Ha van G-ben teljes párosítás, akkor $|A| = |B|$ teljesül, továbbá a teljes párosítás egyúttal fedi az A színosztályt is, így A Hall tétel miatt $|X| \leq |N(X)|$ teljesül minden $X \subseteq A$ ponthalmazra.

2. *Másik irány:* Teljesül az $|A| = |B|$ és a Hall feltétel. Ekkor a Hall tétel miatt G-ben létezik egy A-t fedő M párosítás, és $|A| = |B|$ miatt M fedi B-t is, tehát M teljes párosítás.

Hall tételének bizonyítása:

1. *Szükségesség:* Ha létezik A-t fedő párosítás, akkor minden A-beli pontnak különböző párja van, tehát $X \subseteq A$ esetén $|X| \leq |N(X)|$

2. *Elégségesség:* Tegyük fel, hogy $|X| \leq |N(X)|$ minden $X \subseteq A$-ra. Azt kell igazolni, hogy $\nu(G) \geq |A|$ (így lefogja A-t mert A-n belül nem fut él). Legyen U minimális (azaz $\tau(G)$ méretű) lefogó ponthalmaz, és legyen $U_A = U \cap A$ (azaz a lefogó pontok közül az A-beliek) és $U_B = U \cap B$ (a B-beliek). Mivel U mindent lefog, így $X = A \setminus U_A$-ból induló éleket is lefogja, ezért $N(X) \subseteq U_B$, mert ezeket nem U_A pontjai fogják le, vagyis csak U_B-i lehetnek az őket lefogók. Így $|N(X)| \leq |U_B|$. Ekkor $\nu(G) = \tau(G) = |U| = |U_A| + |U_B| \geq |U_A| + |N(X)| \geq |U_A| + |X| = |A|$. A feltevés (Hall feltétel) és a Kőnig tétel miatt így mivel $\nu(G) \geq |A|$ ezért G-ben létezik A-t fedő párosítás.

$\nu(G)$*:* maximális független élhalmaz (maximális párosítás)
$\tau(G)$*:* minimális lefogó ponthalmaz

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

Javítóutas algoritmus: (páros gráfokra)

1. Kiindulunk egy párosításból (lehet az üres is) és ezt javíthatjuk.
2. Ha már találtunk egy M párosítást, akkor tekintjük az M-hez tartozó segédgráfot: M éleit B-ből A-ba irányítjuk, G többi élét A-ból B-be.
3. Ebben a gráfban egy olyan irányított utat keresünk, amely egy A-beli M szerint fedetlen pontból indul, és ugyancsak M szerint fedetlen B-beli pontba érkezik. Ha találunk ilyen utat, akkor ezen út éleit, amelyek M-ben szerepelnek elhagyjuk M-ből, amelyek pedig nem szerepelnek M-ben azokat bevesszük. Így M elemszámát növeltük. Addig ugrunk vissza a 2. lépésre, amíg találunk javítóutat.
4. Ha már nem létezik több javítóút, M maximális, és megadható egy $|M|$ csúcsot tartalmazó lefogó ponthalmaz is.

Harmadik tétel

Kőnig tételei. Párosítások tetszőleges gráfban. Tutte tétele (csak szükségesség bizonyításával). Gallai tételei.

Kőnig tételei

Definíciók: G gráfra

$\nu(G)$*:* maximális független élhalmaz (maximális párosítás)
$\tau(G)$*:* minimális lefogó ponthalmaz
$\alpha(G)$*:* maximális független ponthalmaz
$\rho(G)$*:* minimális lefogó élhalmaz

Kőnig tétele páros gráfokra: Ha G véges, páros gráf, akkor $\nu(G) = \tau(G)$.

Bizonyítás Menger tételével: Vegyük a G páros gráfot A és B osztályokkal, és vegyünk hozzá két pontot (s, t) úgy, hogy s-t kössük össze az összes A-beli, t-t az összes B-beli ponttal. Legyen ez a G' gráf. Látszik, hogy a G' beli pontdiszjunkt $s-t$ utak száma egyenlő a G-beli független élek számával. (Élen keresztül lesz út, pontdiszjunkt utaknak nincs közös éle) Vagyis $\nu(G) = \kappa_G(s, t)$. G'-ben s és t nem szomszédok $\Rightarrow$ Menger 4 tétele szerint a pontdiszjunkt $s - t$ utak száma megegyezik a minden $s - t$ utat lefogó és s-től és t-től különböző pontok minimális számával. G csúcsainak egy U részhalmaza akkor fogja pontosan le G minden élét, ha U G' minden $s-t$ útját lefogja, vagyis $\tau(G) = \kappa_{G'}(s, t) = \nu(G)$.

Kőnig II. tétele: Ha G véges, páros gráfnak nincs izolált pontja, akkor $\alpha(G) = \rho(G)$.

Bizonyítás: Páros gráfban nem lehet hurokél, így Kőnig előző, valamint Gallai 2. tételéből: $\alpha(G) = n - \tau(G) = n - \nu(G) = \rho(G)$.

Gallai tételei

Gallai tételei: Legyen G n pontú gráf.

1. Ha G-ben nincs hurokél, akkor $\tau(G) + \alpha(G) = n$.

2. Ha G-nek nincsen izolált pontja, akkor $\nu(G) + \rho(G) = n$.

Bizonyítás:

1. Ha egy $U \subseteq V(G)$ lefogó ponthalmaz, akkor $V(G) \setminus U$ független ponthalmaz. Ebből adódik hogy $\tau(G) + \alpha(G) = n$.

2. A $\nu(G)$ diszjunkt él $2\nu(G)$ pontot fog le. A maradék $n - 2\nu(G)$ pont pedig lefogható egy-egy új éllel (hiszen nincs izolált pont), azaz $\nu(G) + n-2\nu(G) = n-\nu(G)$ éllel minden pont lefogható. Innen $\rho(G) \leq n-\nu(G)$, amiből $\nu(G) + \rho(G) \leq n$ adódik.
   Másrészről egy él maximum 2 pontot fog le, ezért egy $\nu(G)$ élei biztosan szerepelnek $\rho(G)$-ben, hiszen ha nem így lenne, csökkenteni lehetne $\rho(G)$-beli elemek számát. A lefedetlen pontok közt pedig nem lehetnek szomszédosak, hiszen akkor az őket összekötő élet bevehetnénk $\nu(G)$-be, viszont

$\nu(G)$ maximális. Ebből következik, hogy minden eddig le nem fogott pontot egy-egy új éllel tudunk lefogni, így $\rho(G) = \nu(G) + (n - 2\nu(G)) = n - \nu(G)$, ez pedig átrendezve a tétel állítása.

Tutte tétele

Tutte tétele: A véges G gráfnak pontosan akkor van teljes párosítása, ha tetszőleges $X \subseteq V(G)$ esetén a keletkező páratlan komponensek száma ($c_p(G-X)$) kevesebb az elhagyott csúcsok számánál. ($c_p(G - X) \leq |X|$)

Bizonyítás (szükségesség): 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 van. Ennek a párosításélnek a másik végpontja így biztosan X-ben van. Tehát minden páratlan komponenshez tartozik egy X-beli pont. Így, ha több a páratlan komponens mint $|X|$, akkor a gráfban nem lehet teljes párosítás.

Berge tétele: A G gráf M párosítása pontosan akkor maximális, ha nem létezik M-hez javítóút.

Petersen tétele: Minden véges 3-reguláris 2-élösszefüggő gráfnak van teljes párosítása.

Negyedik tétel

Gráfok színezése. $\chi(G)$ fogalma, és viszonya $\omega(G)$-hez, illetve $\Delta(G)$-hez, mohó színezés. Mycielski konstrukciója.

Gráfok színezése

Definíció: A G gráf k színnel színezhető, ha minden csúcsa kiszínezhető a k adott szín valamelyikére úgy, hogy bármely két szomszédos csúcs más színű legyen. A G gráf kromatikus száma $\chi(G) = k$, ha G k színnel kiszínezhető, de k-1 színnel már nem.

Tulajdonságok:

1. Ha G k-színezhető, akkor nincs benne hurokél (a definíció szerint nem tudnánk kiszínezni a hurokél végpontját)
2. A G gráf k színezése egy olyan c leképezés, amelyre $c(u) = c(v) \Rightarrow uv \notin E(G)$ teljesül.
3. A G gráf egy (adott színezéshez tartozó) színosztályának csúcsai között nem fut él.

Definíció: 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, amelyre G-nek van k pontú teljes részgráfja, de k+1 pontú már nincs.

Definíció: A G gráfra $\Delta(G)$ a gráf legnagyobb (fokszámú pontjának a) fokszáma.

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

Bizonyítás: n pontú teljes gráf csak n színnel színezhető. G kiszínezésekor G legnagyobb klikkjét is kiszínezzük, vagyis annak a pontszáma alulról becsüli $\chi(G)$-t.
A mohó színezés pedig mutatja, hogy bármely G gráf $\Delta(G)$+1 színnel színezhető.

Mohó színezés: Színezzük G pontjait $v_1, v_2, \ldots, v_n$ sorrendben úgy, hogy az i-edik lépésben v_i-t olyan színnel színezzük, amely nem szerepel v_i kiszínezett szomszédain (csak akkor vegyünk fel új színt, ha v_i-nek van minden eddigi használt színű szomszédja). Mivel v_i-nek legfeljebb $\Delta(G)$ kiszínezett szomszédja lehet, és mindegyik szomszéd legfeljebb 1 színt zár ki, v_i színezésése elvégezhető a $\Delta(G) + 1$ szín valamelyikével, vagyis G $(\Delta(G) + 1)$-színezhető.

Tétel: Minden irányítatlan, véges G gráfra $\chi(G)\cdot\alpha(G) \geq n$, ahol n G csúcsainak száma.

Bizonyítás: Ha G gráfot kiszíneztük $\chi(G)$ színnel, akkor minden színosztály legfeljebb $\alpha(G)$ méretű, vagyis G-t felbontottuk $\chi(G)$db maximum $\alpha(G)$ méretű halmaz úniójára. Ebből következik az állítás.

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

Mycielski konstrukció

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

Bizonyítás: A **Mycielski konstrukció**val. G_k gráf, k paraméter szerinti indukcióval. A $G_k = K_2$ megfelelő gráf, tehát $k = 2$-re az állítás igaz. Tegyük fel, hogy k-ra a G_k gráfot már el tudtuk készíteni. Legyen G_{k+1} az a gráf, amely:

1. $V(G_{k+1}) = \{v_1, v_2, \ldots, v_n\} \cup \{u_1, u_2, \ldots, u_n\} \cup \{\omega\}$, ahol u_i és ω az edigiektől és egymástól eltérő új csúcsok.
2. $E(G_{k+1}) = \{wu_1, wu_2, \ldots, wu_n\} \cup \{v_iu_j, v_ju_i : v_iv_j \in E(G_k)\} \cup E(G_k)$

Azaz kössük össze az összes u-t w-vel, valamint minden G_k-beli él (önmagán kívül) két élért felelős G_{k+1}-ben.
G_{k+1}-ben nincs háromszög, mert az u-k nem szomszédosak, és w nem szomszédos egy v-vel sem. Így $\forall$ lehetséges háromszög legalább két pontja v-beli. A harmadik pont nem lehet v-beli az indukciós feltevés miatt, nem lehet a w sem, mert az egy v-vel sem szomszédos, és u sem lehet, mert a konstrukció alapján egyik u sincs összekötve a neki megfelelő v-vel ($u_iv_i \notin E(G_{k+1})$). Így $\omega(G_{k+1}) = 2$.
Kell még, hogy G_{k+1} (k+1) kromatikus k szerinti indukciót használunk. $k = 2$-re $\chi(K_2) = 2$ miatt az állítás igaz. G_{k+1} kiszínezhető $k+1$ színnel úgy, hogy a v_i-ket egy G_k szerint jó k-színezéssel kiszínezzük, minden u_i-t v_i színére színezünk, w pedig megkapja a $k+1$-edik színt.
Kell, hogy G_{k+1} nem színezhető k-színnel.
Indirekt: Tegyük fel, hogy színezhető. Ekkor vegyünk fel egy jó ilyen k-színezést. Színezzük át az összes w-ével megegyező színű v_i-t u_i színére. Ezáltal minden v_i egy w-ától különböző színt kap. Tehát a G_k pontjai $k-1$ színt kaptak. Viszont tudjuk, hogy G_k kiszínezésére k-1 szín kevés, az indukciós feltevés miatt.
Ebből következik hogy volt két azonos színű szomszédos csúcs, mondjuk v_i és v_j. Ezek az eredeti színezésben különböző színt kaptak, így egyikük (mondjuk v_i) a w-vel azonos színt kapott, és ezért színeztük át az u_i színére. Azonban v_j és u_i is szomszédosak G_{k+1}-ben, tehát eredeti színük különböző volt. Így az átszínezés után sem fordulhat elő, hogy v_i és v_j azonos színt kapott. Ez az ellentmondás igazolja az indukciós állítást, azaz $\chi(G_{k+1}) = k+1$.

Ötödik tétel

Síkba rajzolható gráfok kromatikus száma, ötszíntétel. Algoritmus intervallumgráfok optimális színezésére. Élkromatikus szám: $\chi_e(G)$ viszonya $\Delta(G)$-hez, Vizing-tétel(bizonyítás nélkül)

Gráfok élszínezése

Definíció: A G gráf k-élszínezhető, ha G élei k színnel színezhetőek úgy, hogy szomszédos élei különböző színt kapnak. A G gráf élkromatikus száma $\chi_e(G) = k$, ha G k-élszínezhető, de nem $(k-1)$-élszínezhető.

Definíció: A G gráf élgráfja az az $L(G)$ gráf, aminek a csúcsai G éleinek felelnek meg, és $L(G)$ két csúcsa akkor szomszédos, ha a G megfelelő éleinek van közös végpontja.

G gráf pontosan akkor k-élszínezhető, ha $L(G)$ k-színezhető. Tetszőleges G gráf esetén $\chi_e(G) = \chi(L(G))$

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

Bizonyítás: 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.

Következmény: Tetszőleges G gráfra $\chi_e(G) \geq \Delta(G)$ ($L(G)$-ben a kromatikus számot $\omega(L(G))$ alulról becsüli).

Tétel (Kőnig tétel): Ha G páros gráf, akkor $\chi_e(G) = \Delta(G)$.

Bizonyítás: Létezik olyan H páros gráf, aminek G részgráfja, és H $\Delta(G)$ reguláris. Reguláris, páros gráf pedig élszínezhető a "regularításával", itt $\Delta(G) = r$ (r a regularítás). Keressünk benne egy teljes párosítást, színezzük ki egy színnel, majd vegyük ki a gráfból. Ezt addig ismételjük, amíg készen nem leszünk. (Teljes párosítás létezése Hall-feltételből. Egy színosztály k pont $\rightarrow$ $k \cdot r$ él $\rightarrow$ ebből minden színosztály legfeljebb r szín fogadhat be $\rightarrow$ legalább k pontra van szükség: $|N(X)| \geq |X|$.)

Vizing tétele: Ha G véges, egyszerű gráf, akkor $\chi_e(G) \leq \Delta(G) + 1$

Ötszín-tétel

Négyszín-tétel: Minden egyszerű, síkbarajzolható gráf 4-színezhető.

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

Bizonyítás: Indukcióval. Legfeljebb 3 pontú gráfokra a tétel igaz. Tegyük fel, hogy legfeljebb $n-1$ pontú gráfokra már igazoltuk az állítást. Vegyük az $n(>3)$ pontú gráfot (ami síkbarajzolható és egyszerű). G élszáma legfeljebb $3n-6$, így fokszámösszege maximum $6n-12$. Ezért G-nek létezik egy legfeljebb 5-fokú csúcsa, a v csúcs. Ezt elhagyva a (G-v) gráf az indukciós feltevég miatt 5-színezhető.
Ekkor G-ben ha v fokszáma ≤ 4, akkor a gráfot ki tudjuk színezni 5 színnel (v-nek az 5. színt adva). Ha v fokszáma 5, és minden szomszédja különböző színű, vegyük az 1,3 színek által feszített részgráfot. Ha ebben a gráfban v két szomszédja különböző komponensben van, akkor az egyik komponensben lévő csúcsok színét felcserélhetjük, és így v megkaphatja ezt a színt, vagyis G 5-színezhető. Ha v két szomszédja egy komponensben van az 1,3 színek által feszített részgráfban, akkor létezik olyan út a két csúcs között, amely csak 1-es és 3-as színeket használ. Most tekintsük a 2,4 színek által feszített részgráfot. Ebben a részgráfban v 2 és 4 színű szomszédja biztosan nincsen egy komponensben, hiszen G síkbarajzolhatósága és a 1 és 3 szomszéd között vezető, csak 1,3 színű út miatt a 2 és 4 színű szomszéd között nem vezethet csak 2 és 4 színű csúcsokon át haladó út. Így a két szomszéd a feszített részgráfban biztosan különböző komponensben vannak. Így felcserélhetjük az egyik komponensben lévő csúcsok színét a másik színére, és így lesz v-nek két azonos színű szomszédja, vagyis tudunk neki egy 5. színt adni. Ezzel bizonyítottuk az indukciós lépést. G 5-színezhező.

Intervallumgráf színezése

Definíció: Intervallumgráf: Legyenek az $I_1, I_2, \ldots$ valós intervallumok a G gráf csúcsai, és I_iI_j között pontosan akkor fusson él, ha $I_i \cap I_j \neq \varnothing$.

Intervallumgráf optimális színezése: Mohó színezés algoritmusával. Meghatározunk egy sorrendet, és minden csúcsot olyan színűre színezünk, ami nem mond ellent a korábbi intervallumszínezésnek. Ezt megtehetjük $\omega(G)$ színnel, ahol G az intervallumgráfunk. Ha $\omega(G)+1$ színt kellene használnunk, az azt jelentené, hogy az éppen színezni kívánt intervallumnak már van közös pontja $\omega(G)$ másik intervallummal, ami ellentmondás, hiszen ekkor $\omega(G)$ eggyel több lenne.

Tétel: Ha G intervallumgráf, akkor $\chi(G) = \omega(G)$.

Hatodik tétel

Hálózat, hálózati folyam és vágás fogalma, folyam értéke, vágás kapacitása. Algoritmus maximális folyam és minimális vágás megkeresésére, Ford-Fulkerson tétel, Edmons-Karp tétel (bizonyítás nélkül), egészértékűségi lemma. A folyamprobléma általánosítása.

Hálózatok

Definíció: Hálózatnak nevezünk egy olyan (G, s, t, c) négyest, amelyben G egy irányított gráf, amelynek s és t különböző csúcsai, továbbá G minden e élét jellemzi egy nemnegatív $c(e)$ szám, az él úgynevezett kapacítása.

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

1. $0 \leq f(e) \leq c(e)$ teljesül G minden élére (kapacítást nem lépheti túl)
2. $\sum\{f(uv) : uv \in E(G)\} = \sum\{f(vu) : vu \in E(G)\}$ fennáll G minden s-től és t-től különböző csúcsára. (amennyi befolyik, annyi folyik ki)

Definíció: Az f folyam m_f folyamnagysága vagy folyamértéke az a nettó folyammennyiség, ami s-ből kifolyik: $m_f = \sum\{f(sv) : sv \in E(G)\} = \sum\{f(vs) : vs \in E(G)\}$. (Az s-be befolyó folyammenyiséget le kell vonni!)

Definíció: Legyen X a G csúcsainak egy $s - t$ tartalmazó, de t-től diszjunkt részhalmaza. Az X és $V(G) \setminus X$ között futó élek halmazát (G-ben) a hálózat egy st-vágásának nevezzük. Az X által meghatározott st-vágás kapacítása az X-ből $V(G) \setminus X$-be futó élek kapacításának összege, azaz $\sum\{c(xv) : x \in X \not\ni v \in V(G)\}$.

Tétel: Ha f a (G, s, t, c) hálózat egy folyama, és $s \in X \subseteq V(G) \setminus \{t\}$, akkor $m_f = \sum\{f(xv) : x \in X \not\ni v \in V(G)\} - \sum\{f(vx) : x \in X \not\ni v \in V(G)\}$, valamint $m_f \leq \sum\{c(xv) : x \in X \not\ni v \in V(G)\}$
Vagyis f folyamnagysága meghatározható úgy, hogy egy vágásra X-ből $V(G)\setminus X$-be futó éleken haladó összfolyammennyiségből levonjuk a $V(G) \setminus X$-ből X-be továbbított folyammennyiséget.

Bizonyítás: Felhasználva a folyam két definícióbeli tulajdonságát:
$m_f = \sum\{f(sv) : v \in V(G)\} - \sum\{f(vs) : v \in V(G) \setminus X\} =$
$= \sum_{x \in X} \{f(xv) : v \in V(G)\} - \sum\{f(vx) : v \in V(G)\} =$
$= \sum_{x \in X} \{f(xv) : v \in V(G) \setminus X\} - \sum\{f(vx) : v \in V(G) \setminus X\} =$
$= \sum\{f(xv) : x \in X \not\ni v \in V(G)\} - \sum\{f(vx) : x \in X \not\ni v \in V(G)\}$
$\leq \sum\{c(xv) : x \in X \not\ni v \in V(G)\}$
(Egymás után alkalmazzuk a két definícióbeli tulajdonságot)

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 kapacításával. (Vagyis létezik maximális folyam, és minimális vágás, és ezek egyenlőek.)

Bizonyítás: Javítóutas algoritmus felhasználásával. Legyen f maximális nagyságú folyam. Vezessük be a (G_f, s, t, c_f) hálózatot a $G_f = (V(G), E_f))$ segédgráfon, melyre $E_f : E_f^{elore} \cup E_f^{vissza}$, vagyis G_f-nek vannak előre és visszaélei, ahol egy előreél kapacitása legyen a rajta még "átvihető" mennyiég f szerint, a visszaél kapacitása pedig legyen az élen már átvitt mennyiség f szerint, vagyis:

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

Így az előreéleken még növelhető a folyam, a visszaéleken pedig csökkenthető. Ha tehát van egy P orányított út G_f-ben s-ből t-be ($\Rightarrow$ javítóút), akkor P előreélein ε-nal megnövelve f-et, P visszaéleinek megfordítottjain ε-nal csökkentve f-et egy, a Kirchoff-szabályt teljesítő f'-t kapunk. Ha ε-t alkalmasan választjuk (P út éleinek kapacitásai közül a legkisebbre növelünk), akkor az eredeti kapacitásfeltételek is fennmaradnak, tehát f' folyam lesz, melynek nagysága $m_{f'} = m_f + \varepsilon > m_f$, ellentmondásban van m_f maximalításával.
Ezt a módszert egy kiinduló folyamból (például 0 nagyságúból) egymás után alkalmazva, az f'-kkel tovább haladva előbb-utóbb megkapjuk a maximális folyamot, amennyiben a hálózat kapacitásai egész nagyságúak. Ez a javító utas algoritmus.
Legyen X a G_f-ben (az előbb leírt maximális f-re) az s-ből elérhető pontok halmaza. A fentiek alapján $t \notin X$ azaz X csakugyan st-vágást határoz meg. (Nem tudtuk a folyamot növelni $\rightarrow$ vagyis s-ből t-be eljutni). Mivel X-ből nem lép ki él G_f-ben, ezért minden X-ből $V(G) \setminus X$-be vezető út uv élére $f(uv) = c(uv)$, és minden $V(G) \setminus X$-ből X-be vezető uv élen $f(uv) = 0$. Ha tehát e vágás segítségével határozzik meg az m_f folyamnagyságot, akkor
$m_f = \sum\{f(xv) : x \in X \not\ni v \in V(G)\} - \sum\{f(vx) : x \in X \not\ni v \in V(G)\} = \sum\{c(xv) : x \in X \not\ni v \in V(G)\}$
Ez pedig éppen az X által meghatározott st vágás kapacítása.
Ezek alapján és ha minden él kapacitása egész, az előzőleg leírt javítóutas algoritmus előbb-utóbb a maximális folyamnagyságot adja (a folyammal együtt), hiszen bármely vágáskapacitás felülről korlátoz, és ha a segédgráfon nem tudunk növelni, tudunk mutatni egy a folyamértékkel egyenlő kapacitású vágást a hálózatban. Mivel minden ε-nal növelésnél egy egész értékkel növeljük a folyamot, a maximális folyamértéke is egész lesz.
Ez bizonyítja az alábbi lemmát.

Tétel: Ha a (G, s, t, c) hálózatban minden él kapacitása egész szám, akkor létezik olyan maximális f folyam, amely a G gráf minden élén egész értéket vesz fel.

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

A folyamatprobléma általánosításai:

1. Több forrásból több nyelőbe vezet a folyam, de nincs megkötés arra, hogy melyik forrásból melyik nyelőbe kell érkeznie a folyamnak. Van $s_1, s_2, \ldots, s_k$ forrásunk, és $t_1, t_2, \ldots, t_k$ nyelőnk. Ekkor vegyünk fel egy új s és t csúcsot, majd az s-ből az összes s_i-be irányítsunk egy-egy végtelen kapacitású élet (elég ha több, mint az s_i-ből kimnenő élek összkapacitása), valamint minden t_i-ből egy-egy végtelen kapacitású élet t-be (itt is elég a túlléphetetlen). Ezután legyen s az egyedüli forrás, t az egyedüli nyelő. Így egy általános hálózatot kaptunk.

2. A pontoknak is van kapacitása. Ez a probléma is visszavezethető a szokásos folyamproblémára. Minden kapacitással rendelkező v csúcsból egy v_{be} és v_{ki} csúcsot képzünk, a v-be futó éleket a v_{be} csúcsba, a v-ből kifutó éleket a v_{ki} csúcsból vezetjük. Továbbá vezetünk egy élet a v_{be} csúcsból a v_{ki} csúcsba, amelynek kapacitása a v kapacitása.

3. Ha megengedünk irányítatlan éleket is, akkor úgy vezethetjük vissza a problémát az általánosra, ha minden c kapacitású irányítatlan él helyére felveszünk két ellentétesen irányított c kapacitású élt.
   Ha azt szeretnénk hogy egyszerre mindkét irányba ne haladhasson a folyam, akkor csak olyan folyamokat tekintsünk, ahol legalább az egyik él kapacitása nulla.

Hetedik tétel

Menger pontpárok közötti diszjunkt utakra vontkozó tételei. Többszörös összefüggőség és élösszefüggőség fogalma, Menger vonatkozó tételei.

Diszjunkt utak

Definíció: A G irányított vagy irányítatlan gráf u pontjából v pontjába futó P és Q útjait éldiszjunktnak vagy élidegennek nevezzük, ha $E(P) \cap E(Q) = \varnothing$
Ugyanígy pontdiszjunktnak vagy pontidegennek, ha $V(P) \cap V(Q) = \{u, v\}$
Éldiszjunkt utak maximális száma: $\lambda(u, v)$
Pontdiszjunkt utak maximális száma: $\kappa(u, v)$

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

Menger tételei:

1. Ha u és v a G irányított gráf különböző csúcsai, akkor az élidegen uv-utak ($\lambda_G(u, v)$) 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 maximális száma ($\kappa_G(u, v)$) 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 ($\lambda_G(u, v)$) 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 maximális száma ($\kappa_G(u, v)$) azonos az uv-utakat lefogó, u-tól és v-től különböző csúcsok minimális számával.

Bizonyítás: A lefogó élek, illetve pontok száma mindig legalább annyi, mint a szóban forgó utak száma, hiszen minden ilyen út egy-egy különböző élt, vagy csúcsot tartalmaz a lefogókból. Azt kell így bizonyítani, hogy a lefogó elemek száma legfeljebb annyi, mint a diszjunkt utak száma (vagy fordítva).

1. Vegyük a $(G, u, v, 1)$ hálózatot, ahol minden él kapacitása 1. Legyen ebben f egy maximális nagyságú folyam, és X egy olyan ponthalmaz, amely egy minimális uv vágást határoz meg. Az egészértékűség lemma miatt m_f egész, ez legyen k. Ezenkívül az is igaz, hogy minden élen 1 vagy 0 folyik, és hogy X egy olyan vágást határoz meg, amelynek kapacitása k. Ezt azt jelenti, hogy X-ből pontosan k él lép ki. Ezeket elhagyva nem tudunk $V(G) \setminus X$-be eljutni, tehát ez a k él minden uv-utat lefog. Valamint mivel ez egy minimális vágás volt (és minden kapacitás 1), ez a k lefogó él egy az uv-utakat lefogó minimális számú él. Még azt kell megmutatni, hogy létezik k éldiszjunkt út G-ben. Tekintsük a leírt k nagyságú f folyamot, és legyen E' G azon éleinek halmaza, amelyben 1 egységnyi folyam folyik. A

Kirchoff-szabály miatt ekkor minden u-tól és v-től különböző csúcsra igaz, hogy E' pontosan annyi éle megy bele, mint amennyi kijön belőle. Abból pedig, hogy f nagysága k az következik, hogy u-nak k-val több kiéle van, mint beéle, v-nek pedig fordítva. Vegyük a $G^*(V, E^*)$ gráfot, ahol az E^* élhalmaz E'-n kívül tartalmaz még k db vu párhuzamos élet. Ekkor G^* minden csúcsának megyezik a kifoka, és a befoka. Azokat a csúcsokat ne vegyük figyelembe amelyek izoláltak, a többire pedig igaz, hogy van benne Euler-körséta, az irányított gráfokra vonatkozó Euler-körséta tétel miatt. Ha most elhagyjuk a k párhuzamos élt, ez a komponens k db éldiszjunkt uv-sétára esik szét. Minden ilyen uv-sétából kiválasztható egy-egy uv irányított út, vagyus mutattunk k éldiszjunkt utat. (Kész a legfeljebb ág is) Vagyis az éldiszjunkt irányított uv-utak maximális száma legalább annyi, mint az összes irányított uv utat lefogó élek minimális száma. Ebből adódik Menger 1. tétele.

2. Húzzunk szét minden u-tól és v-től különböző csúcsot G-ben két csúccsá. (x csúcsból beélek $\to x_{be} \to x_{ki} \to$ kiélek) Ezt minden nem u, nem v csúcsra elvégezve az így kapott G' gráfban k éldiszjunkt uv-út pontosan k pontdiszjunkt uv-útnak felel meg G-ben, és viszont. Így Menger 1. tételét alkalmazva G'-re, lesz G'-nek $\kappa_G(u, v)$ éle, amelyek G' minden uv útját lefogják, minden ilyen élnek pedig választható egy nem u, nem v végpontja (G-ben). Így legfeljebb $\kappa_G(u, v)$ jelöltük G-nek, és ezek a pontok minden G-beli uv utat lefognak.

3. Készítsünk G' irányított gráfot G-ből, úgy, hogy G minden élét oda és vissza is irányítjuk. Ekkor Menger 1. tétele miatt G'-ben létezik $\lambda_G(u, v)$ és, ami minden G'-beli uv-utat lefog, mert G'-nek pontosan $\lambda_G(u, v)$ éldiszjunkt uv-útja van. Ez azért van, mert ha G-ben $\lambda_G(u, v)$ éldiszjunkt út van, ezek irányított megfelelői jók lesznek G'-ben valamint ha G'-ben van k darab éldiszjunkt irányított út, akkor van k darab ilyen úgy is, hogy nem használnak ellentétesen irányított éleket. (Ha használnak, akkor egyenértékűek 2 olyannal, amelyek nem használnak $\Rightarrow$ felcserélhetőek) Vagyis G'-ben k darab irányított uv-út, G-ben ugyanennyi éldiszjunkt uv-útnak felel meg. Az 1. Menger tétel miatt létező $\lambda_G(u, v)$ G'-beli él G-beli irányítatlan megfelelője pedig minden G-beli éldiszjunkt uv-utat lefog, és ez az élhalmaz is lefgeljebb $\lambda_G(u, v)$ méretű.

4. Alkalmazzuk itt is a 3. Menger tétel bizonyításbeli konstrukcióját. Látszik, hogy itt a G'-beli irányított pontdiszjunkt uv-utak maximális száma $\kappa_G(u, v)$. A 2. Menger tétel alapján G'-nek $\kappa_G(u, v)$ pontja fogja le ezen utakat. Ezek pedig G-ben is jók lesznek.

Többszörös összefüggőség

Definíció: Az irányítatlan G gráf k-szorosan összefüggő, 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.

Definíció: A G irányítatlan gráf k-szorosan élösszefüggő, ha G összefüggő marad, bárhogyan is hagyunk el belőle legfeljebb $k-1$ élt. A maximális k-t, melyre G k-élösszefüggő marad $\lambda(G)$ jelöli.

Tétel: Egy egyszerű, irányítatlan G grág pontosan akkor k-összefüggő, ha G-nek legalább $k+1$ pontja van, és G bármelykét különböző pontja között létezik k pontidegen út. G pontosan akkor k-élösszefüggő, ha G bámely két különböző pontja között vezet k élidegen út.

Bizonyítás: Az irányítatlan Menger tételekből adódik: ha bármely két pont között van k éldiszjunkt, illetve k pontdiszjunkt út, akkor G nem eshet szét k-nál kevesebb él, illetve pont elhagyásával. (Egyik irány)
Ha G k-élösszefüggő, akkor semelyik két pont közti utakat sem fogja le k-nál kevesebb él (hiszen akkor G szétesne), így Menger 3. tételéből adódik, hogy bármely két pont között létezik k éldiszjunkt út. A pontösszefüggőséghez, ha uv nem szomszédosak adódik a tétel Menger 4. tételéből. (Az előző gondolatmenetből) Ha szomszédosak, hagyjuk el az őket összekötő élet. Ezután Menger 4. tételét használva, majd a végén az elhagyott élet visszahúzva adódik a tétel állítása. (Ha több éllel is össze vannak kötbe, hagyjuk el mindet)
(A 4. tételt úgy használjuk, hogy kiveszzük a gráfból a $\kappa_G(u,v)$ pontot, így szétesik, majd visszahúzzuk az elhagyott élt.)

Menger tétele: Ha G legalább 3 pontú gráf, akkor az alábbi állítások ekvivalensek:

1. G 2-összefüggő
2. G bármely 2 pontján át vezet kör.
3. Ha G-nek nincs izolált pontja, G bármely 2 élén át vezet kör.

Bizonyítás:

- $1 \Rightarrow 2$: G 2-összefüggő, bármely 2 pontja között van 2 pontidegen út $\Rightarrow$ ez egy kör.
- $2 \Rightarrow 1$: A kör tekinthető 2 pontidegen út úniójának, így bármely 2 pont között van két pontidegen út.
- $3 \Rightarrow 2$: Ha u-n és v-n keresztül akarunk kört találni, elég egy u-ra és egy v-re illeszkedő kört találni, ami 3. miatt létezik.
- $1 \Rightarrow 3$: G 2-összefüggő marad, ha két élét felosztjuk 1-1 ponttal. 2. miatt létezik az osztópontokon keresztül kör, ami éppen egy a felosztott éleken keresztüli körnek felel meg.

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

Nyolcadik tétel

Oszthatóság, prímszámok, a számelmélet alaptétele (bizonyítás nélkül). Osztók számának meghatározása. Prímek száma $\pi(n)$ nagyságrendje (bizonyítás nélkül), hézag lehetséges nagysága egymást követő prímek között. Euklidészi algoritmus. Kongruencia fogalma, alapműveletek kongruenciákkal.

Oszthatóság, prímszámok

Definíció: Az a, b egész számokról azt mondjuk, hogy a osztja b-t, illetve b az a többszöröse ($a|b$), ha $b = a \cdot c$ valamely c egész számra. Világos, hogy $n \neq 0$ esetén $\pm 1, \pm n | n$, ezek az n triviális osztói. n nemtriviális osztóit valódi osztóknak nevezzük.

Definíció: A $p \in \mathbb{Z}$ szám felbonthatatlan, ha $|p| \neq 1$ és p-t csak triviális módon tudjuk egészek szorzataként előállítani.

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

Bizonyítás: $|z|$ szerinti teljes indukcióval. $|z| = 2$ esetén z felbonthatatlan, és mint egytényezős szorzat megfelel. Tegyük fel, hogy k-ig már bizonyítottuk. Legyen ekkor $|z| = k + 1$. Ha z felbonthatatlan, akkor z megfelel, ha nem az, akkor z nemtriviálisan felbomlik $z = a \cdot b$ szorzatra, ahol $1 < |a| \leq k$ és $1 < |b| \leq k$. Az indukciós feltevésben a és b is előáll felbonthatatlan számok szorzataként, ezért a szorzatukra, z-re is igaz.

A számelmélet alaptétele: Ha z egy egész szám, és igaz rá, hogy $|z| > 1$, akkor z előáll felbonthatlan számok szorzataként, és a z ilyen előállításai csak a tényezők sorrendjében és előjelében különbözhetnek.

Definíció: A $p \in \mathbb{Z}$ szám prím, ha $|p| > 1$ és teszőleges $a, b \in \mathbb{Z}$-re teljesül, hogy $p|ab \Rightarrow p|a$ vagy $p|b$.

Következmény:

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

Bizonyítás:

1. Tegyük fel, hogy p prím, és p felbomlik $p = a \cdot b$ alakban. Ekkor mivel prím $p|a$ vagy $p|b \Rightarrow$ legyen most $p|a$. Ekkor $a = p \cdot k$ és $p \neq 0 \neq a$ miatt $|p| \leq |a| \leq |a| \cdot |b| = |ab|$. Vagyis $a = \pm p$. Így p bármely felbontása triviális, azaz p felbonthatatlan.

2. Tegyük fel, hogy p felbonthatatlan, és $p|ab$.ekkor $z = \frac{ab}{p}$ egész. Így a z felbonthatatlanok szorzataként történő előállítását p-vel megszorozva ab egy ilyen előállítását kapjuk. A számelmélet alaptétele szerint ekkor ab bármely ilyen felbontásában szerepel a p, vagyis $p|a$ vagy $p|b$ vagy mindkettő. Ez pedig éppen p prímtulajdonságát igazolja.

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

Tétel: 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 $\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1}-1}{p_i-1}$

Bizonyítás: $d|n$-hez tartozik egy $d' = \prod_{i=1}^{k} \frac{p_i^{\alpha_i}}{p_i^{\beta_i}}$, ahol a β_i-k a d kanonikus alakjában szerepelnek. Minden osztóhoz egy kitevősorozat tartozik a számelmélet alaptétele miatt, így minden α_i (α_i+1) értékben befolyásolja a lehetséges szprzatokat $(\alpha_i + 1 \cdot \alpha_i + 2 \cdot \ldots)$

Definíció: 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, ami osztója a-nak és b-nek is.

- a és b relatív prímek, ha $(a, b) = 1$
- a és $b \in \mathbb{Z}$ számok legkisebb közös többszöröse az a legkisebb $n \in \mathbb{N}$ szám, amire $a|n$ és $b|n$ teljesül. Jele $[a, b]$.

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

Bizonyítás: Legyen d a és b közös osztója, azaz $d|a$ és $d|b$. Ekkor $d|a - b$ $(a = d \cdot c_1; b = d \cdot c_2; a - b = d(c_1 - c_2))$ és $d|b$, vagyis d $(a - b)$-nek és b-nek is a közös osztója. Ha pedig $d|(a - b)$ és $d|b$ akkor $d|a - b + b = a$, tehát ekkor d a-nak is és b-nek is osztója, vagyis a és b számok közös osztói ugyanazok, mint $a - b$ és b számoké. Ezek között pedig van legnagyobb.

Következmény: Ha a és b egészek, akkor $(a, b) = (a - b, b) = (a - 2b, b) = (a - kb, b)$.

Euklidészi algoritmus, kongruenciák

Euklidészi algoritmus: a, b egészeknek meghatározza az (a, b) legnagyobb közös osztóját.

Működés: (most legyen $a \geq b$) $(a_0 \geq a_1 \geq \ldots \geq a_i)$
$a_0 = a$ $a_1 = b$ $a_{i+1} = a_{i-1} \bmod a_i$,
vagyis a következő elem mindig az előző elem mostanival osztva vett maradéka.
$(9; 6; 9 \bmod 6 = 3; 6 \bmod 3 = 0)$ (a maradék mindig $0 \leq a_{i+1} \leq a_i$)
Az eljárás akkor ér véget, ha $a_{k+1} = 0$, ekkor $(a, b) = a_k$.

Helyessége: Az algoritmus azért ér véget, mert nemnegatív egészek csökkenő sorozata (az első két elem még lehet egyenlő). Mivel $a_{i+1} = a_{i-1} - q_{i-1}a_i$, ezért $(a, b) = (a_0, a_1) = (a_0 - q_1a_1, a_1) = (a_2, a_1) = (a_1, a_2) = (a_1 - q_2a_2) = (a_2, a_3) = \ldots = (a_k, a_{k+1}) = (a_k, 0) = a_k$

Tétel: Teszőleges $a \geq b$ egész számokhoz léteznek olyan k és l egészek, amelyekre $(a, b) = k \cdot a + l \cdot b$ teljesül.

Bizonyítás: Teljes indukcióval. $a_0 = 1 \cdot a + 0 \cdot b$-re és $a_1 = 0 \cdot a + 1 \cdot b$-re igaz. $a_0, a_1, \ldots, a_i$-re már bebizonyítottuk. $a_{i+1} = a_{i-1} - q_ia_i$. Itt a_i-re és a_{i-1}-re már bebizonyítottuk $\Rightarrow$ a kettő különbsége is egészkombináció.

Tétel: Végtelen prímszám van.

Bizonyítás: $n! + 1$.

Tétel: Tetszőleges $n \in \mathbb{N}$-re létezik olyan N, amire az $N + 1, N + 1, \ldots, N + n$ számok összetett számok.

Bizonyítás: Legyen $N = (n + 1)! + 1$. Ekkor tetszőleges $2 \leq k \leq n + 1$ esetén $k|(n + 1)! + k = N + (k - 1)$, tehát $N + 1, N + 1, \ldots, N + n$ számok mindegyike összetett.

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

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

Nagy prímszámtétel:

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

Tehát x-ig kb. $\frac{x}{\ln x}$ prím van.

$$\pi(n) \approx \frac{n}{\ln n}$$

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

Kongruenciák

Definíció: $a, b, m \in \mathbb{Z}$, $0 < m$ esetén azt mondjuk, hogy a kongruens b modulo $m (a \equiv b(m))$, ha $m|a-b$.

Műveletek:

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 $d|a$ és $d|b$ és $a \equiv b(m)$, akkor $\frac{a}{d} \equiv \frac{b}{d}(\frac{m}{(m,d)})$, azaz kongruencia osztásakor a modulust is osztjuk az osztó és a modulus legnagyobb közös osztójával.

Bizonyítás:

1. Tudjuk, hogy $m|a-b$ és $m|c-d$. Ezért $m|a-b+c-d = a+c-(b+d)$, azaz $a+c \equiv b+d(m)$.
   Az is igaz, hogy $m|c(a-b)+b(c-d) = ac-bd$, 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 $a \equiv b(m)$ felírható $a'd'D \equiv b'd'D(m'D)$ alakban, ami definíció szerint $m'D|a'd'D - b'd'D = (a'-b')d'D$, azaz $m'|(a'-b')d'$. Mivel D az m és a d legnagyobb közös osztója, ezért az $m' = \frac{m}{D}$, $d' = \frac{d}{D}$ számoknak már nem lehet közös prímosztójuk. Tehát $m'|(a'-b')$ is igaz, ami pedig $a' \equiv \_(m')$, azaz $\frac{a}{d} \equiv \frac{b}{d}(\frac{m}{(m,d)})$.

Következmény:

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 az $ad \equiv bd(m)$ kongruenciával.
3. Ha a $d > 0$ rögzített egész, akkor az $a \equiv b(m)$ kongruencia ekvivalens az $ad \equiv bd(m)$ kongruenciával.

Bizonyítás:

1. $\pm k \equiv \pm k(m) \Rightarrow a \pm k \equiv b \pm k(m)$ ha $a \equiv b(m)$
2. Az osztásból visszavezetve: szorozzunk be a $d \equiv d(m)$ kongruenciával, osszuk le d-vel: $\frac{ad}{d} \equiv \frac{bd}{d}(\frac{m}{(m,d)})$
3. $a \equiv b(m) \Rightarrow m|a-b \Rightarrow md|(a-b)d \Rightarrow md|ad-bd \Rightarrow ad \equiv bd(md)$

Kilencedik tétel

Lineáris kongruenciák: a megoldhatóság szükséges és elégséges feltétele, a megoldások száma. Euklidészi algoritmus használata lineáris kongruenciák megoldására.

Lineáris kongruenciák

Definíció: Lineáris kongruencián egy $ax \equiv b(m)$ kongruenciát értünk, ahol a és b adott egészek, m pedig adott pozitív egész. A lineáris kongruencia azt jelenti, hogy meghatározzuk mindazok egészeket, amelyeket x helyébe írva a kongruencia teljesül.

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

Bizonyítás:

1. *Szükségesség:* Legyen $d = (a, m)$, $a = a'd$, $m = m'd$. Ekkor az $ax \equiv b(m)$, ha megoldható, akkor $d|m|ax-b$ és $d|a|ax$, vagyis $d|ax-(ax-b) = b \Rightarrow d|b$.

2. *Elégségesség:* Tegyük fel, hogy $d|b$, azaz $b = b'd$. ($d = (m, d)|b$) Ekkor az $ax \equiv b(m)$ leosztása d-vel ekvivalens lépés, vagyis $a'x \equiv b'(m')$, ezután mivel $d = (m, a)$, ezért $(a', m') = 1$. Az Euklidészi algoritmusból következő tétel miatt ekkor (a', m') felírható $ka' + lm'$ alakban, ahol k és l egészek. Ebben a felírásban k és m' legnagyobb közös osztója 1, hiszen ha nem így lenne, akkor $p|a'k + lm' = 1$ állna. (1-nek nincs prímosztója) Ekkor az $a'x \equiv b'(m')$ kongruencia k-val szorzása ekvivalens átalakítás, hiszen k és m' relatív prímek. Így $a'kx \equiv b'k(m')$. k felírása alapján ekkor $(1-lm')x \equiv b'k(m')$. Ehhez az $lm'x \equiv 0(m')$ kongruenciát hozzáadva azt kapjuk, hogy $x \equiv b'k(m)$. Vagyis a kongruencia megoldásai pontosan azok az egészek, amelyek modulo m' kb'-vel egy maradékosztályba tartoznak. Ekkor a megoldások modulo m szerint: mivel $m = m'd$, ezért minden m' szerinti maradékosztály pontosan d darab m szerinti maradékosztály uniója. A bizonyítás esetében ezek: $x \equiv kb'(m')$, vagyis $x \equiv kb'(m), x \equiv kb' + m'(m), x \equiv kb' + 2m'(m), \ldots, x \equiv kb' + (d-1)m'(m)$.

A tétel bizonyításában leírt módszer az euklidészi algoritmussal dolgozik. A lépések a bizonyítás szerint d-t és k, l-et kell meghatározni.

Egy másik hasonló módszer: Vegyük fel a megoldandó $ax \equiv b(m)$ kongruencia mellé az $mx \equiv m(m)$ kongruenciát. Ez minden x-re jó megoldás. A kettőt kongruenciarendszerként kezelve folytassuk. Hasonlóan az euklidészi algoritmushoz minden lépésben a nagyobb együtthatójú kongruenciából vonjuk le a másik egy többszörösét, hogy annál így már kisebb legyen az együtthatója. Ezután a két kisebb együtthatójú kongruenciával folytassuk, addig amíg 0 együtthatót nem kapunk. Ekkopr az előző kongruencia a megoldás. Ennek együtthatója (a, m) lesz.

Tizedik tétel

Teljes és redukált maradékrendszer fogalma, Euler-féle φ-függvény és kiszámítása (bizonyítás csak prímhatványokra). Euler-Fermat tétel, kis Fermat-tétel.

Lineáris kongruenciák

Definíció: Rögzített $m > 1$ egész esetén az m elemű $T = \{a_1, a_2, \ldots, a_m\}$ halmazt modulo m teljes maradékrendszerének (TMR) nevezzük, ha T minden m szerinti maradékosztályából pontosan egy elemet tartalmaz. Az $R \subset \mathbb{Z}$ halmaz pedig redukált maradékrendszer (RMR) modulo m, ha R minden m-hez relatív prím m szerinti maradékosztályból pontosan egy elemet tartalmaz.
A modulo m RMR méretét, azaz azoknak az m szerinti maradékosztályoknak a számát, amelyik m-hez relatív prím számot tartalmaznak $\varphi(m)$-mel jelöljük.
Más megfogalmazásban:
$\varphi(m)$ = az 1 és m közé (zárt) eső m-hez relatív prímek száma.

Ha m prím, akkor 1 és m között minden egész szám relatív prím m-hez, vagyis $\varphi(m) = m - 1$.

Ha m prímhatvány vagyis p^α valamely p prímre, akkor a és m pontosak akkor relatív prímek, ha $p \not| a$. A p-vel osztható m-nél kisebb számok száma pedig $\frac{m}{p}$. Vagyis $\varphi(m) = p^\alpha - p^{\alpha-1}$.

Ha $(m, n) = 1$ akkor $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

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

Bizonyítás: Az ar_i-k páronként különböző redukált maradékosztályba tartoznak, hiszen ha $ar_i \equiv ar_j(m)$, akkor mivel $(a, m) = 1$ oszthatunk a-val, és $r_i \equiv r_j(m)$, ez pedig ellentmondás különböző i,j-re. Ekkor viszont minden redukált maradékosztályból szerepel elem, a mennyiség miatt. (Kell még, hogy ar_i relatív prím m-hez, ez azért van így, mert $(a, m) = 1$). A TMR-re ez hasonlóan belátható: $at_i \equiv at_j(m) \Rightarrow t_i \equiv t_j(m) \Rightarrow i = j$, valamint $t_i + k \equiv t_j + k(m)$.

Euler-Fermat tétel, kis Fermat-tétel

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

Bizonyítás: Legyen $R = \{r_1, r_2, \ldots, r_{\varphi(m)}\}$ RMR modulo m. Az előző tétel szerint $a \cdot R = \{ar_1, ar_2, \ldots, ar_{\varphi(m)}\}$ is RMR modulo m. Mivel kongruenciákat lehet szorozni, ezért $\prod_i r_i \equiv \prod_i ar_i(m)$, vagyis $\prod_i r_i \equiv a^{\varphi(m)} \prod_i r_i(m)$. Mivel $(m, \prod_i r_i) = 1$, ezért a modulus változtatása nélkül leoszthatunk $\prod_i r_i$-vel, így az $a^{\varphi(m)} \equiv 1(m)$ állítás adódik, ami maga a tétel.

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

Bizonyítás: Euler-Fermat tételből:

$$a^{\varphi(p)} \equiv 1(p) \quad \varphi(p) = p - 1$$
$$a^{p-1} \equiv 1(p) \quad / \cdot a$$

Ha $(a, p) = 1$, akkor

$$a^p \equiv a(p)$$

Ha $(a, p) \neq 1$, akkor p prímtulajdonsága miatt $p|a$ így

$$a \equiv 0(p)$$

$$a^p \equiv 0 \equiv a(p)$$

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

Bizonyítás: $1 \leq a \leq p-1$-hez tartozik $1 \leq b \leq p-1$, hogy $ab \equiv 1(p)$, mert $ax \equiv 1(p)$-nek pontosan 1 megoldása van. Ez lehet önmaga is, de csak 1-re, vagy $(p-1)$-re lesz így. A faktoriális elemeit így párba állítva a szorzat $1^{\frac{p-3}{2}} \cdot 1 \cdot (p-1) \equiv p - 1 \equiv -1(p)$.

Tizenegyedik tétel

Számelmélet és algoritmusok: összeadás, szorzás, maradékos osztás, hatványozás lépésszáma. Modulo m hatványozás polinomiális időben. Prímtesztelés, Carmichael számok. Nyilvános kulcsú titkosítás és digitális aláírás, megavalósítás az RSA módszer segítségével.

Algoritmusok

Algoritmus bonyolultsága: Egy n hosszú bementű algoritmus meghatároz egy $f : \mathbb{N} \to \mathbb{N}$ függvényt, ahol n bemenetre $f(n)$ adja meg az algoritmus lépésszámát. Ha ez a függvény polinomiális az algoritmus jó, míg ha exponenciális akkor rossz.

Algoritmusok lépésszáma: A bemenetek n és m.

- *Összeadás:* Írásbeli összeadás műveletigénye minden helyiértéknél legfeljebb kettő (esetleg átvitt maradék). Így a lépésszám $2 \cdot max(\log n, \log m) < 2 \cdot (\log n + \log m) \Rightarrow$ lineáris $\Rightarrow$ polinomiális (kivonás hasonlóan).
- *Szorzás:* Írásbeli szorzás $\log n$ db összeadással elégezhető, ahol minden összeadandó m egy egyjegyű számmal szorzott többszöröse, egy ilyen szorzás pedig $2 \log m$ lépésben elvégezhető. Így a lépésigény $2(\log n)(\log m) \leq (\log n + \log m)^2$, vagyis polinomiális.
- *Hatványozás:* Az n^m szám számjegyeinek száma $\log n \cdot 2^{\log m}$, vagyis $k \cdot 2^l$, ha k és l a két bemenet hossza. Így a végeredményt még leírni sem tudjuk a bemenet hosszának polinomjával becsült időben.
- *Maradékos osztás:* Az írásbeli osztás elvégezhető polinomiális időben (a soron következő hányados megbecsülése a nehezebb rész), aminek a végén megkapjuk a maradékot.
- *Modulo m hatványozás:* $a^k(m)$ értékét szeretnénk kiszámítani. Írjuk fel k-t kettes számrendszerben, ezután számítjuk ki az n_i számokat úgy, hogy $n_0 \equiv n(m), n_1 \equiv n^2(m), \ldots, n_i \equiv n^{2^i}(m)$ és $0 \leq n_i \leq n - 1$. Ekkor az $n_{i+1} \equiv n_i^2(m)$, vagyis az előzőből a következőt egy szorzással és egy maradékos osztással kaphatjuk, és n_i mérete mindig legfeljebb $\log m$ lesz. Így egy n_i kiszámítása egy legfeljebb $\log m$ nagyságú szám négyzetre emelését, majd egy maximum $2 \log m$ nagyságú maradékos osztását igényli. A szükséges n_i-k kiszámításához ezt $\log k$-szor kell megtenni. Az n^k meghatározását pedig $n^k = \prod_{i=1}^{\infty} n^{k_i 2^i} \equiv \prod_{i=1}^{\infty} n^{k_i}(m)$ 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. Így a mod m hatványozás összességében is polinomiális eljárás.
- *Euklidészi algoritmus:* Polinomiális időben fut. Egy lépés $a_{i+1} = a_{i-1} - q_i a_i$. Egy maradékos osztás, valamint $a_{i+2} \leq \frac{a_i}{2}$ ezért a_0 lépésből végez az eljárás. Így polinomiális.

Prímtesztelés

Prímtesztelés: polinomiális időben $n \in \mathbb{N}$ számról

Fermat-teszt: Euler-Fermat tétel: ha $(k, n) = 1$, akkor $k^{n-1} \equiv 1(n)$, ha n prím.
n árulója: $k \in \mathbb{N}$ szám, ha $k^{n-1} \not\equiv 1(n) \Rightarrow$ n nem prím
n leleplezője: $k \in \mathbb{N}$ szám, ha $(k, n) \neq 1$, itt is igaz hogy $k^{n-1} \not\equiv 1(n)$, hiszen $k \notin$ RMR mod n
n cinkosa: $k \in \mathbb{N}$, ha $k^{n-1} equiv 1(n)$, ha n összetett

Állítás: Ha $q \leq c_1 \leq c_2 \leq \ldots \leq c_l \leq n$ az n szám cinkosai, és a az n egy árulója, akkpr $ac_1, ac_1, \ldots, ac_l$ az n szám páronként (mod n) különböző árulói, vagyis ha van áruló, akkor legalább annyi áruló van, mint cinkos.

Bizonyítás: Ha $ac_i \equiv ac_j(n)$, akkor $(a, n) = 1$ miatt $c_i \equiv c_j^{(n)}$, vagyis $c_i \equiv c_j$, tehát ac_i-k különböző meradéosztályokból valóak. Mivel $a_i^{n-1} \equiv 1(n)$ és $a^{n-1} \not\equiv 1(n)$, ezért $a^{n-1} \equiv (ac_i)^{n-1} \not\equiv 1(n)$, tehát az ac_i-k tényleg árulók.

Így a Fermat-teszt lépései:

- Válasszunk ki egy $0 < k < n$ számot
- Ha k árulója vagy leleplezője n-nek, azaz $k^{n-1} \not\equiv 1(n)$, akkor kész vagyunk, n összetett
- ha k cinkos, akkor n-ről azt valószínűsítjük, hogy prím.

A Fermat-teszt hibázhat, de az előző állítás szerint hibája csak az lehet, ha egy összetett számot prímnek mond. Ha n-nek van árulója, akkor a hiba valószínűsége $\frac{1}{2}$. Így m-szer ismételve az eljárást a hiba valószínűsége $\frac{1}{2^m}$. A többször megismételt Fermat-teszt pedig polinomiális időben működik.

A Fermat-teszt hibája: Csak akkor működik, ha n-nek létezik árulója. Azonban léteznek olyan számok, amelyeknek csak cinkosai és leleplezői vannak. Ezek az álprímek, vagy *Charmichael számok*. Ezeket az ismételt Fermat-teszt is majdnem biztosan prímnek találja.

Miller-Robin teszt: A Fermat-teszt azt ellenőrzi, hogy $k^{n-1} \equiv 1(n)$, azonban a prímekre ennél több is igaz. Ha n prím, akkor $n-1 = 2^t \cdot q$, ahol q páratlan alakban felírva és az $(x+y)(x-y) = x^2 - y^2$ azonosságot többször alkalmazva:

$$k^{n-1} - 1 = k^{2^t q} - 1 = (k^{2^{t-1} q} - 1)(k^{2^{t-1} q} + 1) =$$
$$= (k^{2^{t-2} q} - 1)(k^{2^{t-2} q} + 1)(k^{2^{t-1} q} + 1) = \ldots =$$
$$= (k^q - 1)(k^q + 1)(k^{2q} + 1)(k^{4q} + 1) \ldots (k^{2^{t-1} q} + 1)$$

Tehát ha $n = p$ prím, akkor p a fenti egyenlet jobboldalának valamelyik tényezőjét is osztja, a prímtulajdonság miatt. Így hiába osztható a baloldal n-el, ha a jobboldal egyetlen tényezője sem osztható n-el, n összetett, és k az n szám Charmichael értelemben vett ártulója. Igaz, hogy minden összetett szám redukált maradékrendszerének $\frac{3}{4}$-része Charmichael értelemben vett áruló. Ezért a Miller-Robin teszt egy összetett számról legalább $\frac{3}{4}$ valószínűséggel megállapítja, hogy nem prím. Az algoritmus tényezőnként vizsgál ($k^{2^i q} \equiv^? -1(n)$).

Titkosítás

Nyilvános kulcsú titkosítás: Egyirányú függvények létezésére épít.

Egyirányú függvény: $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ függvény, ha f bijekció, mely hatékonyan számítható, azonban az f^{-1} leképezés kiszámítása, csupán f ismeretében reménytelen.
Elképzelhető, hogy f^{-1} kiszámítására is létezik hatékony eljárás, azonban ennek megtalálása pusztán f ismeretében reménytelen. Az ilyen függvényeket *kiskapus egyirányú függvénynek* nevezzük.

Egy rendszernél rögzítünk egy $\sum$-val jelölt ABC-t: A kódolandó üzenet (M) t betűből áll, azaz $M \in \sum^t$. Ha az üzenet hosszabb, blokkokra vágjuk. Legyenek $\sum^t$ szavai 1 és $|\sum|^t$ közötti természetes számok.
Ekkor a nyilváos kulcsú titkosítás egy olyan kiskapus egyirányú $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ függvény írja le, melyre $n \geq |\sum^t|$. Ezt a leképezést egy nyilvános kulcs segítségével egyértelműen megadjuk, és bárki számára hozzáférhetővé tesszük. Feltesszük továbbá, hogy a címezett (A) képes f^{-1} hatékony kiszámítására, azaz rendelkezik az f^{-1} titkos kulccsal. Ekkor ha küldünk A-nak egy M üzenetet a titkos kulccsal $f(M)$, azt csak ő tudja hatékonyan visszafejteni $f^{-1}(f(M)) = M$. Bárki más azonban, aki nem rendelkezik a titkos kulccsal, nem tudja az üzenet tartalmát visszafejteni.

Digitális aláírás: Minden szereplőnek van egy nyilvános kulcsa $f_A, f_B, \ldots$, egy kiskapus egyirányú függvény, amelynek az inverzét $f_A^{-1}, f_B^-1, \ldots$ csak az egyes szereplők ismerik, vagyis titkosak. Ha A aláír egy M üzenetet, akkor $f_A^{-1}(M)$-et küldi tovább. Erre ráalkalmazva a nyilvános f_A-t bárki láthatja, hogy ő írta-e az M üzenetet, ehhez pedig nincs szükség a titkos kulcsára.

RSA titkosítás

RSA rendszer: ("A" a címzett) "A" választ véletlenszerűen (sokjegyű) p és q prímeket.
$n = p \cdot q \quad m = \varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$ és egy l számot úgy, hogy $0 < l \leq n$ és $(l, m) = 1$. Ezután "A" közhírré teszi a nyilvános kulcsokat: n-t és l-t, a többi titok (p, q, m). Valamint legyen $f(M) = M^l \pmod n$. Ezután, ha valaki az M üzenetet szeretné elküldeni $f(M)$-et küldi. "A" ekkor így fejti vissza az üzenetet: kiszámolja azt a d-t, amelyre $ld \equiv 1(m)$ (vagyis l multiplikatív inverzét (mod n), mivel $d \equiv l^{-1}(m)$). Ez a d a titkos kulcs, mert egy ilyen d van, mert $(l, m) = 1$. Az elküldött M üzenet most $M^l(n) = X$, erre $X^d = (f(M))^d \equiv (X^l)^d = X^{ld} = X^{lm+1} = X^{lm} \cdot X = (X^m)^l \cdot X \equiv 1^l \cdot X \equiv X (\text{mod n})$
Vagyis $f^{-1}(M) = M^d (\text{mod n})$.
Ezek a műveletek hatékonyak, hiszen a mod n havényozás (f és f^{-1}), a szorzás (n és m), a maradékos osztás és az Euklidészi algoritmus (d) is polinomiális időben végezhetőek.

Az RSA-hoz tartozik még a p és q kiválasztásának módszere. Ezt egy maghatározott számjegyű véletlen szám generálásával történuk, amelyről a hatékony prímtesztelési algoritmussal (Fermat-teszt, Miller-Robin teszt) döntjük el, hogy prím-e, és ezt addig ismétlik, amíg kettő prímet nem találnak.
A kiskapu abból származik, hogy n-t nem tudjuk közvetlenül faktorizálni, így m-et sem tudjuk meghatározni, azonban p és q ismeretében d is hatékonyan számítható.
Ha l-t jól választjuk, akkor pedig l ismeretéből d meghatározása hasonlóan nehéz, mint n-ből p és q-é.

Tizenkettedik tétel

Művelet fogalma, csoport, Abel-csoport. Példák: csoportok számokon, mátrixokon, rajzok szimmetriacsoportja, diédercsoport. Példák véges, végtelen, kommutatív és nem kommutatív csoportra mind a négy lehetséges variációban.

Művelet

Definíció: A H halmazon értelmezett n-változós műveleten egy tetszőleges $f : H^n \to H$ leképezést értünk, azaz midnen, H elemeiből képzett rendezett n-eshez H-nak egy bizonyos elemét rendeljük.

Lényegében: Ha a H halmazon értelmezett, akkor H elemeiből képezzen H-ba, azaz ne vezessen ki H-ból. (Skaláris szorzás nem művelet, mert a skalár és a a vektor nem ugyanott vannak.)

Asszociativitás: A H halmazon értelemzett $*$ művelet asszociatív, ha tetszőleges $x, y, z \in H$-ra $x * (y * z) = (x * y) * z$.

Kommutativítás: Ugyanígy egy H halmazon értelmezett $*$ művelet kommutatív, ha tetszőleges $x, y \in H$-ra $x * y = y * x$.

Példák:

- $\mathbb{R}$-en a $+$ asszociatív és kommutatív.
- $\mathbb{R}^+$-on a hatványozás egyik sem.
- $\mathbb{R} \to \mathbb{R}$ valós függvények kompozíciója asszociatív, de nem kommutatív.
- $\mathbb{R}$-en vett számtani közép kommutatív, de nem asszociaítív.

Félcsoport, csoport

Definíció: Az $S = \langle H, * \rangle$ struktúra félcsoport, ha $*$ művelet H-n és asszociatív. Ha kommutatív is, akkor Abel-félcsoport.

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

Megjegyzés: Ha az S struktúra $*$ műveletének van egységeleme, akkor egyetlen egységeleme van.

Bizonyítás: Tegyük fel hogy $e, e' \in H$ egységelemek, ekkor $e = e * e' = e'$.

Definíció: Ha az $S = \langle H, * \rangle$ struktúrában $e \in H$ a $*$ művelet egységeleme, akkor h' a h inverze a $*$ műveletre, ha $h, h' \in H$ és $h * h' = h' * h = e$.

Definíció: Az $S = \langle G, * \rangle$ struktúra csoport, ha

1. S félcsoport
2. a $*$ műveletnek létezik egységeleme
3. minden $g \in G$-re létezik g inverze a $*$ műveletre.

Az $S = \langle G, * \rangle$ struktúra Abel-csoport, ha csoport és a $*$ művelet kommutatív is.

Példák:

1. $\langle \mathbb{R}, + \rangle, \langle \mathbb{Z}, + \rangle \langle \mathbb{R} \setminus \{0\}, \cdot \rangle, \langle \mathbb{R}^{n \times k}, + \rangle$ csoportok, ahol $\mathbb{R}^{n \times k}$ jelöli az $n \times k$-as valós mátrixokat.
2. Jelölje $\mathbb{Z}_n$ a modulo n maradékosztályok halmazát, és $+_n$ a modulo n összeadást. Ekkor $\langle \mathbb{Z}_n, +_n \rangle$ csoport. A 0 maradékosztály az egységelem.
3. A $\mathbb{Z}_n$ halmazon a modulo n szorzás is asszociatív művelet, és az 1 maradékosztály egységeleme, azonban a 0 maradékosztálynak nincs inverze. Így $\langle \mathbb{Z}_n, \cdot_n \rangle$ egységelemes félcsoport. Ha $\mathbb{Z}_n^*$ jelöli az RMR(n)-eket, akkor viszont $\langle \mathbb{Z}_{n^*}, \cdot_n \rangle$ csoport. Inverz az Euler-Fermat tételből. (Kommutatív is!)
4. Nim összeadás a nemnegatív egészeken Aben-csoport (a Nim $b = a_2$ bitenként XOR b_2).
5. $\langle \mathbb{R}^{n \times k}, \cdot \rangle$ félcsoport, az $\langle \mathbb{R}^{n \times k}$ szimmetrikus mátrixok, $\cdot \rangle$ Abel-félcsoport (az előző félcsoport részfélcsoportja). (ha det = 0 nincs inverze, így nem csoport)

   Részcsoport: $S = \langle H, * \rangle$ csoport az $S' = \langle H', * \rangle$ az S részcsoportja, ha $H' \subseteq H$ és a $*$ művelet H'-n is.

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

   Bizonyítás: Tegyük fel hogy x és y a $g \in G$ inverzei, és e az egységelem. Ekkor $x = xe = x(gy) = (xg)y = ey = y$.
6. $\langle \mathbb{R}_*^{n \times n}, \cdot \rangle$ csoport, ha $\mathbb{R}_*^{n \times n}$ jelöli a nemnulla determinású mátrixokat, és $\cdot$ a mátrixszorzás.

Definíció: Két csoport izomorf, ha van köztük művelettartó bijekció, azaz létezik egy $\phi : G \to H$ bijekció, amire tetszőleges $g, g' \in G$ esetén $\phi(g \cdot g') = \phi(g) * \phi(g')$ ($\cdot$ G-n, $*$ H-n művelet)
Tetszőleges G csoport részcsoportjainak metszete is G részcsoportja.

Diédercsoport: Szimmetriák alkotta csoportok: Legyen X egy halmaz, és tekintsük $f : X \to X$ bijekciónak egy olyan F nem üres halmazát, ami zárt a kompozícióra, vagyis $f, g \in F$ estén $f \circ g \in F \forall x \in X$, továbbá minden $f \in F$ bijekció f^{-1} inverze is F-ben van. A $\circ$ asszociatív, valamint a kritériumok miatt van egység és inverz, így e miatt $\langle F, \circ \rangle$ csoport. Az egységelem az id identitás. (identikus leképezés)

Az egyik lefgontosabb példa a fenti szimmetriacsoportra a D_n diédercsoport, amikoris X a sík egy szabályos n oldalú sokszöge, és D_n csoport elemei az X egybevágóságai, melyek az X sokszöget fixen hagyják. A csoportművelet az egybevágóságok egymás utáni elvégzése. Ilyen egybevágóságok:

- identikus leképezés: id
- a sokszög középpontja körüli $\frac{2\pi}{n}$ szögű f forgatás
- a sokszög egy szimmetriatengelyére való tükrözés t

Diédercsoport $n > 2$-re nem kommutatív. Az f és a t szimmetriák a sokszög minden szimmetriáját generálják. A D_n diédercsoportnak $2n$ eleme van.
$t \circ t = id, f^n = id, f \circ t = t \circ f^{n-1}$

Például (a szabályos háromszögre) D_3 diédercsoport elemei: $id, f, t, f^2, t \circ f^2 = t', t \circ f = t''$

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

Példák csoportokra:

- véges:
  - kommutatív: $\langle (0, 1, \ldots, n-1), +_n \rangle$, $\langle RMR(n), \cdot_n \rangle$
  - nem kommutatív: Diédercsoportok, Permutációcsoportok
- végtelen
  - kommutatív: $\langle \mathbb{R}, + \rangle, \langle \mathbb{Z}, + \rangle, \langle \mathbb{R} \setminus \{0\}, \cdot \rangle$
  - nem kommutatív: $\langle \mathbb{R}_n^{n \times n}, \cdot \rangle, \langle f : \mathbb{R} \to \mathbb{R}, \circ \rangle$

$\mathbb{R}_n^{n \times n}$ a nemnulla determinánsú $n \times n$-es mátrixok.

Tizenharmadik tétel

Elem rendje, részcsoport, ciklikus csoport, példák. Mellékosztály fogalma, példák, Lagrange tétele, következménye az elemek rendjére vonatkozóan. A szimmetrikus csoport. Csoportok izomorfiája, Cayley tétele (bizonyítás nélkül).

Ciklikus csoport, elemek rendje

Definíció: Két csoport (G és H) izomorf, ha van köztük művelettartó bijekció, azaz létezik $\phi : G \to H$ bijekció, amire tetszőleges $g, g' \in G$ esetén $\phi(g \cdot g') = \phi(g) * \phi(g')$.

Definíció: A G csoport H részhalmaza a G részcsoportja ($H \leq G$), ha H maga is csoport a G csoportműveletére.

Definíció: Tetszőleges $K \subseteq G$ által generált $\langle K \rangle$ csoport a G csoport K-t tartalmazó részcsoportjainak metszete. (Ekkor $\langle K \rangle$ a G egy részcsoportja.)

Definíció: Az olyan csoportot, amit valamely eleme generál, ciklikus csoportnak nevezünk.
A G csoport g elemének rendje a g által generált $\langle g \rangle$ részcsoport elemszáma.

Az elem rendjének definíciója úgy is kimondható, hogy a legkisebb n szám, amelyre $g^n = e$. Ha ugyanis létezik ilyen n, akkor $g^{-1} = g^{n-1}$(inverze), és a $g, g^2, g^3, \ldots, g^n$ elemek különbözőek (ha $g^i = g^j$ akkor $g^{i \cdot j} = e$), 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 G végtelen, akkor a generátorelemek semelyik hatványa sem egységelem, mert egyébként csak véges sok elemet generálna. $(g, g^2, g^3, \ldots)$
Ha pedig $g \in G$ generátor, akkor G minden eleme előáll $g^i (= g \cdot g \cdot g \cdot \ldots \cdot g[i\text{-}szer])$ alakban, ahol $i \in \mathbb{Z}$

Definíció: A csoport rendje a csoport elemszáma. (=egy generátor rendjével)

Tétel: A véges ciklikus csoportot az elemszáma izomorfia erejéig mehatározza. (G és H $g \in G, h \in H$ generátorok $\Rightarrow \varphi(g^i) = h^i$ izomorfia)

Példák:

- *Véges:* Az n elemű ciklikus csoport jele C_n. $C_n \cong \mathbb{Z}_n (izomorf)$, ahol $\mathbb{Z}_n$ a $\langle \mathbb{Z}_n, + \rangle$, ahol $\mathbb{Z}_n$ a modulo n maradékosztályok halmaza. Így leírható minden ciklikus csoport.
- *Végtelen:* Ha G végtelen ciklikus csoport, akkor a g generátorelem egyik hatványa sem egységelem, mert egyébként g véges csoportot generálna. Mivel a g által generált e, g^i, g^{-i} elemek részcsoportot alkotnak, ezért g éppen a részcsoportot generálja, így ez a részcsoport maga a G. Vagyis minden végtelen ciklikus csoport a $\langle \mathbb{Z}, + \rangle$ csoporttal izomorf.

Tétel: Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás: Legyen G ciklikus csoport, melynek generátoreleme g, és legyen $H \leq G$ részcsoport. Tekintsük a minimális $0 < k$-t, amire $g^k \in H$, ekkor g^k generálja H-t, vagyis H ciklikus, mert g^k generálja az e, g^{ik}, g^{-ik} elemeket tetszőleges pozitív egész i-re. Tegyük fel, hogy $g^l \in H$-t nem generálja. Ekkor $l = ak+r$ innen: $g^k, g^l \in H$ $g^l \cdot ((g^k)^{-1})^a = g^{ak+r} \cdot g^{-ak} = g^{ak+r-ak} = g^r \in H \Rightarrow$ H ciklikus.

Definíció: Az S_n szimmetrikus csoport $\{1, 2, \ldots, n\}$ halmaz permutációi alkotta csoport a függvénykompozíció műveletre nézve.
Ha $i \in \{1, 2, \ldots, n\}, \sigma \in S_n$ akkor az $i, \sigma(i), \sigma^2(i), \ldots$ elemek (vagyis amelyekbe σ i-t elviszi) i σ szerinti orbitját alkotják. Az orbitot alkotó sorozatban az elemek ciklikusan ismétlődnek, azaz $\sigma^{j+k}(i) = \sigma^j(i)$, ahol k az orbit mérete. Így az $(i, \sigma(i), \sigma^2(i), \ldots, \sigma^{k-1}(i))$ ciklikussorrend a σ permutáció egy ciklusa. Ez alapján:

Tétel: Minden permutáció felírható diszjunkt ciklusok szorzataként.

Tétel: Ha a 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.

Definíció: Transzpozíció egy olyan permutáció, aminek a fixpontjain kívül csak egy kételemű ciklusa van.

Tétel: A transzpozíciók generálják az S_n szimmetrikus csoportot.

Bizonyítás: $(i_1, i_2, \ldots, i_k)$ előáll az $(i_1, i_k)(i_1, i_{k-1}) \ldots (i_1, i_2)$ transzpozíciók szorzataként.

Tétel: S_n generálásához legalább n-1 transzpozíció kell. $(1, 2), (1, 3), \ldots, (1, n)$ jó is.

Definíció: Az S_n szimmetrikus csoport részcsoportját permutációcsoportnak nevezzük.

Cayley tétele: Minden véges G csoport izomorf egy alkalmas permutációcsoporttal.

Bizonyítás alapja: G n-edrendű, elemei $\{1, 2, 3, \ldots, n\}$. Ekkor G minden g elemének megfeleltethető egy σ_g permutáció: $\sigma_g(i) = g \cdot i$ (A $\cdot$ a G csoportművelete)

Lagrange tétel

Definíció: 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 $a \in gH(q \in Hg)$, akkor a-t a $gH(Hg)$ mellékosztály reprezentánsának nevezzük.

Példák: 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 többszörösét jelöli. Egy adott $k \in \mathbb{Z}$ esetén a G csoport k szerinti baloldali mellékosztálya, a $k + n\mathbb{Z}$ halmaz lesz, vagyis azon egészek, amelyek k-val kongruensek modulo n.

Megfigyelés: Legyen $H \leq G \ni g, g'$. Ekkor:

1. $g \in Hg$
2. $g' \in Hg \Rightarrow Hg = Hg'$
3. $Hg = Hg'$ vagy $Hg \cap Hg' = \varnothing$
4. $|H| = |Hg|$

Bizonyítás:

1. $e \in H \Rightarrow g = e \cdot g \in Hg$
2. $g' \in Hg \Rightarrow g' = h \cdot g$ valamely $h \in G$-re. Ekkor $Hg' = H(hg) = (Hh)g \subseteq Hg$ és $g = h^{-1}g'$, amiből az előző elgondolás alapján $Hg \subseteq Hg'$
3. Ha $\exists g^* \in Hg \cap Hg'$, akkor $Hg = Hg^* = Hg'$ (2) miatt.
4. Ha $h, h' \in H$ és $h = h'$ akkor $hg \neq h'g$, ezért $h \to hg$ bijekció H és Hg között.

Következmény:
Lagrange tétel: Ha $H \leq G$, akkor $|H| \mid |G|$. Speciálisan, G bármely g elemének rendje ($\langle g \rangle \leq G$) osztja G rendjét.

Bizonyítás: Az előző megfigyelésből G előáll néhány H szerinti (jobboldali) mellékosztály uniójaként és minden mellékosztály $|H|$ elemet tartalmaz.

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

Következmény: Minden prímrendű csoport ciklikus.

Bizonyítás: Bármely $l \neq g \in G$ elem a Lagrange tétel miatt generálja G-t $\Rightarrow$ G ciklikus.

Tizennegyedik tétel

Gyűrű, ferdetest és test fogalma. Nullosztómentes gyűrű, ferdetest nullosztómentessége. Példák: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$

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

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

Bizonyítás: A disztributivítás miatt $0 = 0a + (-0a) = (0 + 0)a + (-0a) = 0a + 0a - 0a = 0a$. Innen $-ab = -ab + 0 = -ab + 0b = -ab + (a + (-a))b = -ab + ab + (-a)b = (-a)b$. $a0$ és $-ab = a(-b)$ ugyanígy.

Példák:

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ gyűrűk. $\mathbb{N}$ nem az, mert az összeadásra nem csoport (nincs inverz).
2. $n \in \mathbb{N}$-re $(n\mathbb{Z})$ is gyűrű.
3. mod m maradékosztályok is gyűrűk (m-enként)
4. $n \times n$-es mátrixok is gyűrűt alkotnak $(\mathbb{Q}, \mathbb{R}, \mathbb{C})$-n
5. egész együtthatós polinomok is
6. a Gauss egészek $(a + bi$ ahol $a, b \in \mathbb{Z})$ is
7. H halmaz hatványhalmata a szimmetrikus különbségre és a metszetre.

Definíció: Az R gyűrűben az $a \neq 0$ elem nullosztó, ha létezik olyan $0 \neq b \in R$, amire $ab = 0$. Az R gyűrű nullosztómentes, ha nincs benne nullosztó. Az R gyűrű integritási tartomány ha kommutatív és nullosztómentes.

Példák:

1. $n\mathbb{Z}$ kommutatív és nullosztó mentes (tehát integritási tartomány)
2. $\mathbb{Z}_n$ nem integritási tartomány, ha n összetett (van $ab \equiv 0(n)$), azonban az, ha n prím.
3. Boole gyűrű minden valódi részhalmata nullosztó, mert $A \cap (H \setminus A) = \varnothing$

Definíció: Az R gyűrű részgyűrűje az $\langle R, \{+, \cdot\}\rangle$ olyan részstruktúrája, ami gyűrű. $(n\mathbb{Z}, \mathbb{Z}$-re)

Definíció: A T gyűtű ferdetest, ha $\langle T \setminus \{0\}, \cdot \rangle$ csoport. Ha a szorzás kommutatív is, akkor T test.

Példák:

1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ testek.
2. Ha p prím, akkor $\mathbb{Z}_p$ test, aminek a szokásos jelölése $\mathbb{F}_p$, ha m nem prím, akkor $\mathbb{Z}_m$-ben van nullosztó, így nem test.
3. A valós polinomok hányadosteste:
   $\mathbb{R}(x) = \{\frac{p}{q} : p, q \in \mathbb{R}[x], q \neq 0\}$. A műveletek $\frac{p}{q} + \frac{r}{s} = \frac{ps+rq}{qs}$, illetve $\frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs}$
4. Ha $\{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$ halmaz is test $\sqrt{2}$ helyett $\sqrt{t}$ is jó, ahol $0 < t \in \mathbb{Q}_+$

Tétel: Minden test nullosztómentes. Minden ferdetest is.

Bizonyítás: $a \cdot b = 0$

- Ha $a = 0$ akkor kész
- Ha $a \neq 0$, akkor $a \cdot b = 0$, $a^{-1} \cdot a \cdot b = 0a^{-1}$, $b = 0$.

Tétel: Minden véges integritási tartomány test.

Bizonyítás: A végesség szükséges, hiszen $n\mathbb{Z}$ integritási tartomány, de nem test. Integritási tartományon a szorzás kommutatív $\Rightarrow$ csak az egységelem és az inverz létezése kell. Legyen R véges integritási tartomány, és legyen $0 \neq a \in R$. Ha $ab = ab'$, akkor $0 = ab + (-ab') = ab + a(-b') = a(b + (-b'))$, és a nullosztómentesség miatt $b + (-b') = 0$, vagyis $b = b'$, így az $ar_1, ar_2, \ldots$ elemek mind különbözőek ahol $R = \{r_1, r_2, \ldots\}$. Ekkor R végessége miatt a teljes halmaz előáll.
$R = \{ar : r \in R\}$. Így van olyan r is, amelyre $ae = a$. Ekkor viszont $ab = (ae)b = a(eb) = a(be)$, azaz $0 = a(be) + (-ab) = a(be) + a(-b) = a(be + (-b))$, ahol a nullosztómentesség miatt $be = eb = b$. Tehát e egységelem a szorzásra R-en. $R\forall$ eleme előáll ar alakban (így er alakban is) amire $ar = e$, tehát bármely $0 \neq a$-nak létezik inverze.