Euler- és Hamilton körök

(1) Egy összefüggő G gráfban $\exists$ Euler-kör $\Leftrightarrow$ G $\forall$ pontjának foka páros

(2) Egy éf. G gráfban $\exists$ Euler-út $\Leftrightarrow$ G $\forall$ pontjának foka páros, 2 kivétellel

(1) Ha G-ben $\exists$ Hamilton-kör és $X \subseteq V(G)$ tetsz. $\Rightarrow G-X$ összefüggő komponenseinek a száma $\leq |X|$

(2) Ha G-ben $\exists$ Hamilton-út és $X \subseteq V(G)$ tetsz. $\Rightarrow G-X$ éf. komp. száma $\leq |X|+1$

szükséges feltételek

(Dirac) Ha G egy n-pontú egyszerű gráf és $\boxed{\forall x \in V(G) \text{-re } d(x) \geq \frac{n}{2}} \Rightarrow \exists$ G-ben Hamilton-kör

(Ore) Ha G egy n-pontú egyszerű gráf és $\boxed{\forall x,y \in V(G) \text{-re, ha } d(x)+d(y) < n,}$ akkor $\boxed{\{x,y\} \in E(G)} \Rightarrow \exists G$-ben Hamilton-kör

VAGY: $\{x,y\} \notin E(G) \Rightarrow d(x)+d(y) \geq n$; $\forall x,y \in V(G)$-re

elégséges feltételek

Gráfok színezése

- $\forall G$ gráfra $\chi(G) \geq \omega(G)$
- $\chi(G)=1 \Leftrightarrow E(G)=\emptyset$ és $V(G) \neq \emptyset$
- $\chi(G)=2 \Leftrightarrow G$ páros gráf ($K_{3,3}$ is páros gráf!)
- G páros $\Leftrightarrow$ $\forall$ körének a hossza páros
- $\exists G_2, G_3, G_4 \dots$ gráfsorozat, melynek $\forall$ tagjára teljesül, hogy $\omega(G_k)=2$ és $\chi(G_k)=k$ ($k \geq 2$ egész): (Mycielski-konstrukció)
- $\forall G$ gráfban $\chi(G) \leq \Delta(G)+1$

(Brooks) Ha G egyszerű, összefüggő; G nem teljes és nem egy páratlan kör $\Rightarrow \chi(G) \leq \Delta(G)$

- $\forall$ egyszerű, síkbarajzolható gráfra $\chi \leq 4$ (4-szín tétel)

Perfekt gráfok, ellátogatás, PERT-módszer

(Lovász) G perfekt $\Leftrightarrow \overline{G}$ perfekt

(erős perfekt gráf tétel) G perfekt $\Leftrightarrow \nexists$ benne C_{2k+1}, $\overline{C_{2k+1}}$ feszített részgráfként ($k>1$)

- **Minden** intervallumgráf perfekt.
- $\Delta(G) \leq \chi_e(G)$

(Vizing) $\Delta(G) \leq \chi_e(G) \leq \Delta(G)+1$ $\forall G$ egyszerű gráfra.

- G erősen éf. $\Rightarrow \nexists$ fonás és $\nexists$ angyal [VIGYÁZAT: $\not\Leftarrow$]
- Egy irányított gráfban van irányított kör $\Leftrightarrow$ G pontjai nem bonthatók emeletekre.

Párosítások

(K.K.)

(Hall) Egy páros gráfban létezik $\forall F$-beli pontot lefedő párosítás $\Leftrightarrow \forall X \subseteq F$-re $|N(X)| \geq |X|$

(Frobenius) G páros gráfban $\exists$ teljes párosítás
$\Leftrightarrow$ 1) $|F|=|L|$
2) $\forall X \subseteq F$-re $|N(X)| \geq |X|$

Jelölések: τ (tau): lefogó pontok minimális száma
α (alfa): független pontok maximális száma
ϱ (ró): lefogó élek minimális száma
ν (nű): független élek maximális száma

- $\exists$ teljes párosítás $\Leftrightarrow \nu(G) = \frac{|V(G)|}{2}$
- $\chi_e \cdot \nu \geq e$, vagy $\frac{e}{\nu} \leq \chi_e \leq e$
- $\chi \cdot \alpha \geq n$, vagy $\frac{n}{\alpha} \leq \chi \leq n$
- $\forall G$ gráfban $\boxed{\nu(G) \leq \tau(G)}$ $\boxed{\alpha(G) \leq \varrho(G)}$

(König) Ha G páros $\Rightarrow \nu(G) = \tau(G)$ és ($\nexists$) $\alpha(G) = \varrho(G)$ (ha $\nexists$ izolált pont G-ben)

(Gallai) (1) $\alpha(G) + \tau(G) = n$ (ha G-ben $\nexists$ kunkedli)
(2) $\nu(G) + \varrho(G) = n$ (ha G-ben $\nexists$ izolált pont)

(Tutte) Egy (nem feltétlenül páros) G gráfban $\exists$ teljes párosítás $\Leftrightarrow \forall X \subseteq V(G)$-re $c_p(G-X) \leq |X|$, ahol $c_p(H)$ jelenti a H gráfban a páratlan pontszámú összefüggő komponensek számát.

Hálózati folyamok

- $\exists$ javító út s-ből t-be a H_f-ben $\Leftrightarrow f$ nem volt max.

(Ford-Fulkerson/max-flow-min-cut) $\boxed{\max_{\forall f} m(f) = \min_{\forall Q} c(Q)}$

(Edmonds-Karp) Ha a javító eljárás során $\forall$ lépésben egy min. élszámú $s \to t$ irányított út mentén javítunk, akkor az össz. lépésszám $\leq c \cdot n^5$

(egészértékűségi lemma) (G, s, t, c) és $\forall e$ élre $c(e)$ egész szám – ekkor:
1) $\max m(f)$ is egész
2) ez a maximum olyan folyammal is elérhető, melyben $\forall$ élen $f(e)$ egész

Menger-tételek, többszörös összefüggőség

(1) $\vec{G}$-ben s-ből t-be vezető éldiszjunkt irányított utak max. száma = az s-ből t-be vezető összes irányított utat lefogó élek min. száma.

(2) $(s,t) \notin E(\vec{G})$; $\vec{G}$-ben s-ből t-be vezető pontdiszjunkt irányított utak max. száma = az s-ből t-be vezető összes irányított utat lefogó pontok min. száma.

(3) G-ben s és t között haladó éldiszjunkt utak max. száma = az s és t között vezető összes utat lefogó élek min. száma.

(4) $\{s,t\} \notin E(G)$; G-ben s és t között haladó pontdiszjunkt utak max. száma = az s és t között vezető összes utat lefogó pontok min. száma.

(5) G-ben $\exists k$ db éldiszjunkt út bármely két pont között $\Leftrightarrow G$ k-szorosan él-összefüggő.

(6) G-ben $\exists k$ db pontdiszjunkt út bármely két pont között $\Leftrightarrow G$ k-szorosan pont-összefüggő.

- $k=2$, $|V|\geq 3$ esetén ...; $k\geq 3$, $|V|>k$ esetén. – tételek.

(Dirac) Ha $k\geq 2$ és G k-szorosan pont öf. $\Rightarrow$ tetsz. $x_1, x_2 \dots x_k \in V(G)$-hez $\exists K$ ör, hogy $x_1, x_2 \dots, x_k \in V(K)$.

Extremális gráfelmélet

(Mantel) Egy n csúcsú háromszögmentes (egyszerű) gráf-nak max. $\left\lceil \frac{n}{2} \right\rceil \cdot \left\lfloor \frac{n}{2} \right\rfloor$ éle lehet.

(Turán) Ha G olyan n csúcsú egyszerű gráf, ami nem tartalmaz $K_r - t$, akkor $|E(G)| \leq |E(T_{r-1}(n))|$. Továbbá: egyenlőség csakis akkor áll, ha $G \cong T_{r-1}(n)$.

Számelméleti alapok

- számelmélet alaptétele
- prímek száma végtelen
- $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_m^{\alpha_m}$ felbontású szám osztóinak száma: $(\alpha_1+1)(\alpha_2+1)\dots(\alpha_m+1)$

  osztóinak összege: $\frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \dots \frac{p_m^{\alpha_m+1}-1}{p_m-1}$
- $\forall k \in \mathbb{N}$-re $\exists k$ egymást követő prím, melyek között $\geq k$ összetett szám van.

(Csebisev sejtés) Nyilvánvaló, hogy $\exists$-e végtelen sok olyan p prím, amire $p+2$ is prím.

(Bertrand-tétele) n és $2n$ között mindig van prím.

(Goldbach sejtés) Minden páros szám felírható két prím összegeként.

(Dirichlet tétele) Ha $(a,b)=1$, akkor végtelen sok $a \cdot k + b$ alakú prím van.

(prímszámtétel) Legyen $\pi(n)$ az n-nél kisebb prímek száma. Ekkor: $\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$

(Green–Tao tétel) $\forall k \in \mathbb{N}$-re $\exists k$ hosszú prímekből álló számtani sorozat.

Kongruenciák

- $\left.\begin{matrix} a \equiv b \ (m) \\ c \equiv d \ (m) \end{matrix}\right\} \Rightarrow$ (1) $a \pm c \equiv b \pm d \ (m)$; (2) $ac \equiv bd \ (m)$; (3) $a^k \equiv b^k \ (m)$ ($k \geq 1$ egész)
- $ac \equiv bc \ (m) \Leftrightarrow a \equiv b \ \left(\frac{m}{(m,c)}\right)$
- $ax \equiv b \ (m)$ megoldható $\Leftrightarrow (a,m) \mid b$; és ha megold-ható $\Rightarrow$ mo.-ok száma mod m: (a,m).

(Wilson) $\boxed{p \text{ prím esetén } (p-1)! \equiv -1 \ (p)}$

TMR és RMR, Euler–Fermat-tétel

- ha $m = p$ (prímszám) $\Rightarrow \varphi(p) = p-1$
- $\varphi(p^2) = p^2 - p$
- $\varphi(p^k) = p^k - p^{k-1}$
- $\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q)$ ($p \neq q$ két prím)
- Ha $(a,b)=1 \Rightarrow \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$
- $\boxed{\text{Ha } n = \prod_{i=1}^{k} p_i^{\alpha_i} \Rightarrow \varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) = n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)}$

- $\{x_1, x_2, \dots x_t\}$ egy TMR mod $m \Leftrightarrow$
  1) $\forall i \neq j$-re $x_i \not\equiv x_j \ (m)$
  2) $t = m$
- $\{x_1, x_2, \dots x_t\}$ egy RMR mod $m \Leftrightarrow$
  1) $\forall i \neq j$-re $x_i \not\equiv x_j \ (m)$
  2) $t = \varphi(m)$
  3) $\forall i$-re $(x_i, m) = 1$
- Legyen $d(a,m)=1$. Ha egy mod m TMR vagy RMR minden elemét a-val megszorozzuk, is.mét egy mod m TMR, ill. RMR-t kapunk.

(Euler–Fermat) Ha $m>1$ tetszőleges egész szám és a tetszőleges olyan szám, melyre $\boxed{d(a,m)=1}$, akkor $\boxed{a^{\varphi(m)} \equiv 1 \ (m)}$

(Kis Fermat) Tetszőleges p prímszáma és tetsz. a egész számra $\boxed{a^p \equiv a \ (p)}$

- Legyen $ax \equiv b \ (m)$ és tfh. $d(a,m)=1$. Ekkor $a^{\varphi(m)} \equiv 1 \ (m)$, ezért a megoldás: $x \equiv b \cdot a^{\varphi(m)-1} \ (m)$

Csoportelméleti alapok

Egy H halmazt a $*$ művelettel csoportnak nevezünk, ha:
1) $*$ asszociatív 2) $\exists$ neutrális elem 3) $*$ invertálható

– szimmetriacsoport, rendje, elem rendje, csoport rendje

- Véges csoportban $\forall$ elem rendje véges.

(Lagrange) Legyen G véges, $H \leq G$. Ekkor H rendje osztja G rendjét.

- $\forall$ véges rendű csoportban $\forall$ elem rendje osztója a csoport rendjének.

– diéder csoport, ciklikus csoport

- Ciklikus csoport részcsoportja is ciklikus.
- Minden prímrendű csoport ciklikus.

Szimmetrikus csoportok ... (+mellékosztály, normálosztó, faktorcsop.)

(Cayley) Minden véges csoport előáll alkalmas szimmetrikus csoport valamely részcsoportjaként.

- Legyen H a G-nek egy valódi részcsoportja, legyen $h \in H$, $a \notin H \Rightarrow h*a \notin H$. (jobboldali mellékosztály ...)
- $(b \notin (H \cup (H*a)) \Rightarrow H*b)$ Nemcsak $H \cap (H*a) = \emptyset$ és $H \cap (H*b) = \emptyset$, hanem $(H*a) \cap (H*b) = \emptyset$ is.
- Ha G véges $\Rightarrow$ H és a jobboldali mellékosztályai lefedik G-t $\Rightarrow |H|$ osztója $|G|$-nek
  ↳ (Lagrange) Ha G véges és ~~$\forall$~~ $x \in G$ tetsz. $\Rightarrow$ $o(x)$ osztója $|G|$-nek
- Kommutatív csoportban $\forall$ részcsoport normálosztó
- Ha G tetsz. és $|H| = \frac{1}{2}|G| \Rightarrow H$ normálosztó
- $a' \in H*a$, $b' \in H*b \Rightarrow a'*b' \in H*(a*b)$

Aritmetikai algoritmusok bonyolultsága (+RSA)

- Ha $d = (a,m)$, akkor d előáll a és m egész együtthatós lineáris kombinációjaként, és ezt polinom idő alatt meg is találhatjuk.

Gyűrűk, testek

- $\mathbb{C}$ és $\mathbb{K}$ között, ill. $\mathbb{C}$ és $\mathbb{R}$ között nincs újabb test.

(Frobenius) $\mathbb{C}$-n túl $\nexists$ bővebb kommutatív test.
Kvaternión-nál bővebb test nincs.

- Köztes testek: $\exists T$ test, hogy $\mathbb{Q} \subset T \subset \mathbb{R}$. (pl. $\mathbb{Q}[\sqrt{2}]$)
- Galois-tételek