

Feltétlenül tudni kell a **félkövéren** szedett fogalmakat, tételeket ill. algoritmusokat definiálni, helyesen kimondani, ill. leírni. A **bekeretezett** állításokat bizonyítottuk, az **aláhúzottakat** nem. A vizsgán az anyag értő ismeretét kérjük számon, az elégséges osztályzathoz bizonyítást nem kell tudni.

1. Leszámlálási alapfogalmak: **permutációk, variációk és kombinációk (ismétlés nélkül és ismétléssel)** például, **kiszámításuk**, binomiális együtthatók közti összefüggések, **a binomiális tétel**.
2. Gráfelméleti alapfogalmak: **pont, él, fokszám**. Egyszerű gráf, részgráf, feszített részgráf, izomorfia, élsorozat, séta, út, kör, **összefüggő gráf**, komponens. **Gráfok fokszámösszege**, erdő, **fa**, fák egyszerűbb tulajdonságai: **két elsőfokú pont**, **fák (erdők) élszáma**.
3. **Feszítőfa létezése**, **minimális költségű feszítőfa**, **Kruskal algoritmus**, **ennek helyessége**.
4. Legrövidebb utakat kereső algoritmusok (**BFS, Dijkstra, Ford, Floyd**), **ezen algoritmusok helyessége**. legrövidebb utak fája Bejárásokkal kapcsolatos fogalmak: bejárési fa, faél, előreél, visszaél, keresztél. **Legszélesebb utak** keresése irányítatlan gráfban: Módosított Kruskal algoritmus, **helyessége**.
5. **Mélyégi keresés** és alkalmazásai (élek osztályozása, mélyégi számozás, befejezési számozás, fa-, előre-, vissza- és keresztélek, **irányított kör létezésének eldöntése DFS-sel**), **alapkörrendszer**. Aciklikus (irányított kört nem tartalmazó) irányított gráfok (DAG-ok), **jellemzésük a topologikus sorrenddel**, topologikus sorrend keresése, **PERT-módszer**, kritikus utak és tevékenységek.
6. **Euler-séta és körséta**, **létezésének szükséges és elégséges feltétele**. **Hamilton-kör és út** létezésére szükséges, ill. elégséges feltételek: **komponensszám ponttörlések után** ill. **Dirac, Ore tételei**.
7. **Gráfszínezés, kromatikus szám, klikkszám**, **alsó és felső korlát** a kromatikus számra. Síkgráfok kromatikus száma: **négyszíntétel**, **ötszíntétel**.
8. Hálózati folyamatok: **hálózat, folyam, folyammagyság (avagy folyamérték), st-vágás, st-vágás kapacitása**. **Ford-Fulkerson tétel**, javító utas algoritmus (előre- és visszaélek). **EgÉR lemma**, Edmonds-Karp tétel, illusztráció. Általánosított hálózatok visszavezetése szokásos hálózatra.
9. **Páros gráfok**, **definíciók ekvivalenciája** **Párosítások** (páros és nem páros gráfban), teljes párosítás, adott ponthalmazt fedő párosítás, **Hall, Frobenius és Kőnig tételei**, alternáló utas algoritmus maximális párosítás keresésére. **Lefogó és független pont- ill. élhalmazok**, az **ezekből származó gráfparaméterek** (τ, α, ρ, ν), **triviális egyenlőtlenségek**, **Gallai két tétele**.
10. **Síkbarajzolhatóság**, gömbre rajzolhatóság, tartomány, sztereografikus projekció. Külső tartomány nem kitüntetett volta. Az **Euler-féle poliédertétel és következményei**: egyszerű, síkbarajzolható gráfokon **felső korlát az élszámra**. **Kuratowski gráfok**, **síkbarajzolhatósága**, **soros bővítés**, **Kuratowski-tétel** **könnyű iránya**.
11. **Oszthatóság, legnagyobb közös osztó**, **euklideszi algoritmus**, prímek és felbonthatatlan számok, a számelmélet alaptétele, **kanonikus alak**, **osztó, lnko kanonikus alakja**, **osztók száma**, nevezetes tételek prímszámokról: **prímek száma**, **prímek közti hézag**, **prímszámtétel**.
12. **Kongruencia fogalma**, **műveletek kongruenciákkal**. Teljes és redukált maradékrendszer, az **Euler-féle φ -függvény**, **$\varphi(n)$ kiszámítása**. Az **Euler-Fermat tétel** és a **kis Fermat-tétel**. **Lineáris kongruenciák** **megoldhatósága** és konkrét módszer a megoldásra.
13. Algoritmusok bonyolultsága (inputméret, lépésszám az inputméret függvényében, polinomidejű algoritmus), döntési problémák. **P, NP, co-NP** bonyolultsági osztályok, feltételezett viszonyuk, példa ilyen problémákra. Polinomiális visszavezethetőség (Karp-redukció), **NP-teljesség**, **Cook-Levin tétel**, nevezetes **NP-teljes** problémák: **SAT, HAM, 3-SZÍN, k-SZÍN, MAXFTN, MAXKLIKK**.
14. Számelméleti algoritmusok: **alpműveletek**, (modulo m) **hatványozás** és az **euklideszi algoritmus lépésszáma**. **Prímtesztelés, Fermat-teszt. Nyilvános kulcsú titkosítás, digitális aláírás**. Az RSA titkosítási módszer (Az üzenetből számok képzése, p és q prímek generálása, n, m kiszámítása, e és d választása, titkos és nyílt adatok, kódoló és dekódoló függvények, **dekódolás működik**).