

SZÁMELMÉLET ÉS ALKALMAZÁSAI

Tételsor, 2015.

1. A Fermat- és a Mersenne számok prímosztói (1.2.4 és 1.2.6. tételek bizonyítása, az 1.2.5. és 1.2.7. tételek megfogalmazása).
2. Prímtesztek az 1.2.8.- 1.2.13. tételek ismertetése, pseudoprímek)
3. A nyilvános kódú titkosítások, az RSA rendszer működése, biztonsága.
4. Véges egyszerű lánc törtek (a 2.2.1. és 2.2.2. tételek).
5. A végtelen egyszerű lánc törtek formális definíciója, a (p_n) és (q_n) sorozatok (a 2.3.1. - 2.3.3. lemmák).
6. A végtelen egyszerű lánc törtek létezése (a 2.3.4. - 2.3.6. tételek).
7. Az irracionális számok lánc tört előállítás (a 2.3.7. tétel és a 2.3.8. lemma).
8. Periódikus lánc törtek (a 2.4.1. tételből annak igazolása, hogy minden periódikus lánc tört kvadratikusan irracionális).
9. Diofantikus approximáció, irracionális számok approximációja (a 3.1.1. - 3.1.3.1.4. tételek).
10. Lánc törtek alkalmazása kéthatározatlanos lineáris diofantoszi egyenletek megoldására.
11. A Pell-egyenlet, megoldása lánc törtek segítségével (a 3.3.1.- 3.3.4. tételek).
12. Maradékosztálygyűrűk egységcsoportja (a 4.1.1 -4.1.3. tételek).
13. Az algebrai számok approximációja (a 3.5.1. tétel).
14. A Gauss-egészek gyűrűje, irreducibilis faktorizáció (a 4.2.1. - 4.2.4. tételek).
15. A Gauss-egészek gyűrűjének prímelemei (a 4.2.5. - 4.2.8. tételek).
16. Euler-egészek (5.2.1. - 5.2.3. tételek).
17. Kvadratikusan testek, irreducibilis faktorizáció egészeik gyűrűjében (a 5.3.1. - 4.3.2. tételek)
18. A valós számok erős approximációja, az erősen approximálható valós számok irracionálisok (az e erősen approximálható, és az 6.1.1. és 6.1.2. állítás).
19. Az e transzcendens szám (a bizonyítás alapgondolata, előkészületek) (az 6.1.5. és 6.1.7. lemmák bizonyítása).
20. Az e transzcendens szám (a bizonyítás alapgondolata, az m_i és ε_i számok tulajdonságai, az 6.1.8. lemma bizonyítása).
21. Az e transzcendens szám (az 6.1.9. lemma és az 6.1.10. tétel).
22. A Riemann-féle ζ függvény és alkalmazása a prímek száma, reciprokaik sora divergenciájának bizonyítására (az 6.2.1. és 6.2.2. tétel).

Megjegyzés. A tételjegyzékben számmal jelölt tételeket a vizsgán részletesen bizonyítani kell, de az anyag többi részéről is tájékozottnak kell lenni (abból is kérdezhetek, ha szigorú bizonyítást nem is).