Számelmélet tematika

Főtárgy esetén az alábbiak közül kettőt, melléktárgy esetén egyet kell választani.

1. Kombinatorikus számelmélet: A Ramsey-tételkör alkalmazásai, Schur-tétel, Van der Waerden-tétel, Hales–Jewett-tétel. Szemerédi számtani sorozatokra vonatkozó tételei. Szita módszerek és alkalmazásaik. Brun-szita, a „nagyobb" szita. Schnirelmann-sűrűség, a prímszámok bázist alkotnak. Kneser-tétel, Mann-tétel. Primitív sorozatok. Additív és multiplikatív Sidon-sorozatok. Algebrai eszközök felhasználása a kombinatorikus számelméletben. A polinom-módszer és a kombinatorikus nullhelytétel alkalmazásai, Erdős–Ginzburg–Ziv-tétel és általánosításai.

Irodalom:
A. Sárközy, C. Pomerance: Combinatorial Number Theory, In: Handbook of Combinatorics I., 20. fejezet; MIT Press, 1995.
A. Geroldinger, I. Ruzsa: Combinatorial Number Theory and Additive Group Theory; Advanced Courses in Mathematics-CRM Barcelona, 2009.
R.L. Graham, B.L. Rothschild, J.H. Spencer: Ramsey-Theory; 2nd ed., Wiley & Sons, 1990.
H. Halberstam, H.E. Richert: Sieve methods; Dover, 2011.
H. Halberstam, K.F. Roth: Sequences; Springer, 1983.
T. Tao, V.H. Vu: Additive Combinatorics; Cambridge University Press, 2010.

2. Additív Számelmélet: Összeg és különbséghalmazok szerkezete. Ruzsa-távolság, additív energia. A Plünnecke-tétel és alkalmazásai. A Balog–Szemerédi–Gowers-tétel. Freiman-homomorfizmus, Freiman tételei és alkalmazásaik. Az Erdős–Fuchs-tétel. A Hardy–Littlewood-módszer és alkalmazásai, Waring-probléma, Goldbach-sejtés, Vinogradov-tétel, Roth-tétel.

Irodalom:
A. Geroldinger, I. Ruzsa: Combinatorial Number Theory and Additive Group Theory; Advanced Courses in Mathematics-CRM Barcelona, 2009.

H. Halberstam, K.F. Roth: Sequences; Springer, 1983.
M.B. Nathanson: Additive Number Theory I.: The Classical Bases; Springer, 1996.
M.B. Nathanson: Additive Number Theory II.: Inverse Problems and the Geometry of Sumsets; Springer, 1996.
T. Tao, V.H. Vu: Additive Combinatorics; Cambridge University Press, 2010.
R.C. Vaughan: The Hardy-Littlewood Method; Cambridge University Press, 1997.

3. Analitikus Számelmélet: Számelméleti függvények. Modern prímszámelmélet, prímszámtétel. Prímek számtani sorozatokban. Addditív és multiplikatív karakterek, Dirichlet-karakterek, Dirichlet L-függvények. A zeta-függvény, Riemann-sejtés. Exponenciális összegek, Weyl és Van der Corput módszerei. Kloostermann-összegek. Valószínűségi számelmélet. Turán–Kubilius-egyenlőtlenség, Erdős–Kac-tétel.

Irodalom:
H. Davenport: Multiplicative Number Theory; Springer, 2000.
A. Ivic: The Riemann Zeta-Function; Dover, 2003.
A.A. Karatsuba: Basic Analytic Number Theory; Springer, 1993.
E. Kowalski, H. Iwaniec: Analytic Number Theory; American Math. Soc., 2004.
H.L. Montgomery, R.C. Vaughan: Multiplicative Number Theory I.: Classical Theory; Cambridge University Press, 2007.
S.J. Patterson: An Introduction to the Theory of the Riemann Zeta-Function; Cambridge University Press, 1988.
G. Tenenbaum: Introduction to Analytic and Probabilistic Number Theory; Cambridge University Press, 1995.

4. Algebrai Számelmélet: Algebrai számok, algebrai egészek. Dedekind-gyűrűk, ideálok, faktorizáció, kapcsolat a számelmélet alaptételével. Tört-ideálok, egész zártság, diszkrimináns. Kvadratikus és körosztási testek. Osztálycsoport, osztályszám végessége. Dirichlet egység tétele. Elágazáselmélet, p-adikus számok, értékelések. Diofantikus egyenletek.

Irodalom:
H. Cohen: Number Theory: Volume I.: Tools and Diophantine Equations; Springer, 2007.
H. Cohen: Number Theory: Volume II.: Analytic and Modern Tools; Springer, 2007.
A. Fröhlich, M.J. Taylor: Algebraic Number Theory; Cambridge University Press, 1991.

G.J. Janusz: Algebraic Number Fields; American Math. Soc., 2005.
D. Marcus: Number Fields; Springer, 1977.
J. Neukirch: Algerbaic Number Theory; Springer, 2010.
P. Ribenboim: Classical Theory of Algebraic Numbers; Springer, 2001.

5. Moduláris Formák: Moduláris forma definíciója, csúcsformák. Eisenstein-sorok, Poincaré-sorok. Hecke-operátorok, Hecke-karakterek, Hilbert-moduláris formák. A Rankin–Selberg-módszer. Artin L-függvények és a Langlands-funktorialitás.

Irodalom:
D. Bump: Automorphic Forms and Representations; Cambridge University Press, 1998.
F. Diamond, J. Shurman: A First Course in Modular Forms; Springer, 2005.
H. Iwaniec: Topics in Classical Automorphic Forms; AMS, 1997.
T. Miyake: Modular Forms; Springer, 2006.
G. Shimura: Introduction to the Arithmetic Theory of Automorphic Functions; Princeton University Press, 1994.
G. Shimura: Modular Forms: Basics and Beyond; Springer, 2012.

6. Osztálytestelmélet: Csoportok kohomológiája, a Tate-csoport. Provéges csoportok kohomológiája, Galois-kohomológia: Additív elmélet, Hilbert 90. tétele, Brauer-csoportok. Lokális osztálytestelmélet. Lokális reciprocitási tétel. Egzisztenciatétel. Lokális testek Brauer-csoportja. Lokális testek Abel-bővítései, elágazó részcsoportok és konduktorok. Globális osztálytestelmélet. Idélek és idélosztályok, idélosztályok kohomológiája. Artin reciprocitási tétele.

Irodalom:
E. Artin, J. Tate: Class Field Theory; AMS Chelsea, 2009.
J. Neukirch: Algebraic Number Theory; Springer, 2010.
J. Neukirch: Class Field Theory; Springer, 2013.
J. W.S. Cassels, A. Fröhlich: Algebraic Number Theory; Academic Press, 2010.
G.J. Janusz: Algebraic Number Fields; American Math. Soc., 2005.
A. Weil: Basic Number Theory; Springer, 1995.

7. A Számelmélet kriptográfiai alkalmazásai Nyilvános kulcsú kriptográfiai protokollok: Diffie–Hellman-elv, RSA-séma, ElGamal titkosító algoritmus. Prímtesztelés. Fermat, Solovay–Strassen, Miller–Rabin prímtesztelő algoritmusok. AKS-algoritmus. Faktorizációs módszerek. Kvadratikus

szita, számtest szita. Diszkrét logaritmus probléma, index kalkulus algoritmus. Elliptikus görbék alkalmazása titkosításra, prímtesztelésre, faktorizációra, diszkrét logaritmus keresésére.

Irodalom:

H. Cohen: A Course in Computational Algebraic Number Theory; Springer, 1993.
N. Koblitz: A Course in Number Theory and Criptography; Springer, 1994.
A.J. Menzes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography; CRC Press, 1997.
R.A. Mollin: RSA and Public Key Cryptography; Chapman & Hall/CRC, 2003.
A.K. Lenstra, H.W.Jr. Lenstra: The Development of the Number Field Sieve; Springer, 1993.
D.R. Stinson: Cryptography: Theory and Practice; CRC Press, 2006.
L.C. Washington: Elliptic Curves: Number Theory and Cryptography; Chapman & Hall/CRC, 2008.