Some familiar topics in Number Theory

A student can do a research project in any of the areas listed below. The list below is not exhaustive; students may contact relevant faculty members based on their interests. This may involve lectures in the second year, or a reading course with discussion, as advised by the faculty members.

Algebraic Number Theory:

Algebraic numbers and algebraic integers, Norm and trace, Algebraic number fields, Integral bases, Monogenety of algebraic number fields, Discriminant of algebraic number fields. Quadratic number fields, Cyclotomic number fields.

Divisibility, UFD, PID, Euclidean domain in algebraic number fields.

Ideal divisors, Fractional ideals, Dedekind domain, Ideal class Groups. Finiteness of ideal class groups.

Units in algebraic number fields, Kronecker's theorem, Minkowski bound, Dirichlet's unit theorem, Cyclotomic units, Algebraic integers lying on the unit circle.

Splitting of rational primes in algebraic number fields, Dedekind criterion for ramification. Kummer-Dedekind theorem on splitting of rational primes, Ramification and discriminant. Decomposition group and inertia groups in a Galois extension over $\mathbb{Q}$, Frobeinus element, Dedekind theorem. State the density theorems of Frobenius and Cebotarev, some of their applications.

Absolute values and completions of number fields.

Textbooks:

1. I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, Chapman and Hall/CRC, 2015.
2. A. Frohlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge University Press, 1998.
3. P. Pollack, *Conversational Introduction to Algebraic number theory*, American Mathematical Society, 2019.
4. G. J. Janusz, *Algebraic Number Fields*, American Mathematical Society, 1996.
5. D. A. Marcus, *Number Fields*, Universitext, Springer, 2018.

Analytic Number Theory:

Introduction to arithmetic functions and Dirichlet series, Summation formulas: Euler-Maclaurin, Poisson summation etc. Riemann Zeta function, Functional equation and Analytic continuation, zeros

of Riemann Zeta function. Non-vanishing of Riemann Zeta function at $\Re(s) = 1$ and Prime number theorem. Dirichlet characters and Gauss sums, Dirichlet L-function, Functional equation and zeros, Primes in arithmetic progressions. Elementary sieve methods, Bilinear forms and the large sieve. Introduction to holomorphic modular forms.

Textbooks:

1. H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Colloquium Publications, **53**, American Mathematical Society, 2004.
2. J. P. Serre, *A Course in Arithmetic*, GTM, **7**, Springer-Verlog, 1973.
3. M. Ram Murty, *Problems in Analytic Number Theory*, GTM, **206**, Springer-Verlog, 2008.
4. M. Ram Murty, M. Dewar and H. Graves, *Problems in the theory of Modular Forms*, IMSC Lecture notes series -1, HBA, Delhi, 2015.

Discrete Mathematics:

Advanced Counting: Stirling numbers of the first and second kind, Pigeon hole principle, generalized Pigeon hole principle and its applications, Erdos - Szekere's theorem on monotone subsequences, Ramsey theorem. Theorem of Hilbert, Dirichlet's theorem on rational approximations. Erdos-Gnizburg-Ziv theorem, Inclusion exclusion principle and its applications. Derangements, Permutations with forbidden positions, restricted positions and Rook polynomials.

Recurrence Relations: The Fibonacci sequence, linear homogeneous and non-homogeneous recurrence relations. Proof of the solution of linear homogeneous recurrence relations with constant coefficient in case of distinct roots and when they have repeated roots, iteration and induction. Ordinary generating functions, exponential functions for counting combinations with and without repetitions, applications to counting, and the use of generating functions for solving homogeneous and non-homogeneous recurrence relations. Catalan numbers.

Polya's method of Counting: Equivalence relations and orbits under the permutation group action. Orbit stabilizer theorem, Burnside lemma and its applications, Cycle index, Polya's formula, Applications of Polya's formula. Theorem of J. P. Serre on Burnside lemma and its applications.

Basic Graph Theory technique: Basic graph theory, Handshaking problem, Graphs and matrices, Planar graphs, Hall's marriage theorem, Kneser's theorem.

Textbooks:

1. A. Tucker, *Applied Combinatorics*, John Wiley & Sons, Inc., New York, 1995
2. P. J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, 1994.
3. S. M. Cioaba and M. Ram Murty, *A first course in Graph theory and Combinatorics*, Texts Read. Math., 55 Hindustan Book Agency, New Delhi Springer, Singapore, 2022.

Local Fields:

Non-archimedean absolute values and topological properties, Ostrowski's theorem, the field of p-adic numbers $\mathbb{Q}_p$, the ring of p-adic integers $\mathbb{Z}_p$ and its properties, Hensel's lemma, the Teichmüller map, quadratic forms, Hasse-Minkowski theorem. Elementary analysis in $\mathbb{Q}_p$: Laurent series, continuity, derivatives and convergence conditions of various Laurent series, Strassmann's theorem and its consequences, exponential and logarithm maps and their convergence results. Extensions of $\mathbb{Q}_p$: extension of absolute values for finite extensions of $\mathbb{Q}_p$, construction and properties of $\mathbb{C}_p$ - the algebraic closure of $\mathbb{Q}_p$, Eisenstein irreducibility criterion over $\mathbb{Q}_p$, the ramification and the residue indices for finite extensions of $\mathbb{Q}_p$, roots of unity in $\mathbb{Q}_p$, the p-th cyclotomic polynomial and its irreducibility, construction of the cyclotomic extension of $\mathbb{Q}_p$, ramified and unramified extensions of local fields, Krasner's lemma, Analysis on $\mathbb{C}_p$, Higher ramification groups and solvability of finite Galois extensions of p-adic fields.

Textbooks:

1. F. Q. Gouvêa, *p-adic numbers*, Springer, 1997. J-P Serre, *Local fields*, Springer, 1979 (Chapters I-V).
2. J.W.S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, 1967.
3. Yvette Amice, *Les nombres p-adiques*, Presses Universitaires de France, 1975.
3. G. Bachman, *Introduction to p-adic numbers and valuation theory*, Academic press, 1964.

Galois Cohomology of elliptic curves:

Profinite groups, cohomology and homology of pro-p groups, restriction, corestriction homomorphisms and functoriality properties, induced modules, cup products, statements of the spectral sequence

for group extensions and the inflation-restriction exact sequence, p-cohomological dimension, strict cohomological dimension, interpretations of the dimensions of $H^1(G, \mathbb{Z}/p\mathbb{Z})$ and $H^2(G, \mathbb{Z}/p\mathbb{Z})$ in terms of generators and relations of the pro-p group G.

Elliptic Curves (general overview with statements of main results and examples): Definition of elliptic curves using generalized Weierstrass equations, Tate-module, torsion points, Weil pairing, Hasse theorem for elliptic curves over finite fields, elliptic curves over local fields, definitions of good and bad reduction, elliptic curves over $\mathbb{Q}$, weak Mordell-Weil theorem, Mordell-Weil theorem. Kummer sequence of elliptic curves via cohomology, definitions of Selmer groups and Shafarevich-Tate groups over number fields, the exact sequence connecting the p-primary Selmer group with the p-part of the Shafarevich-Tate group and the Mordell-Weil group, cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, Selmer groups and Shafarevich-Tate groups over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and their arithmetic properties.

Textbooks:

1. J-P Serre, *Galois cohomology*, Springer, 1997.
2. L. Washington, *Elliptic Curves: Number Theory and Cryptography*, (second edition), Chapman and hall/CRC, 2008.
3. J. Silverman, *Rational points on Elliptic curves*, Springer, 2015.
4. J. Silverman, *The arithmetic of Elliptic curves*, Springer, 2009.
5. J. Coates and R. Sujatha, *Galois cohomology of elliptic curves*, a publication of Tata Institute of Fundamental Research, 2010.

Introduction to Elliptic curves:
Elliptic curve and rational points, group law, elliptic curves over a finite field, elliptic curves over complex numbers, elliptic curves over local and global fields, Mordel-Weil theorem, Selmer group, and Tate-Shafarevich group.

Textbooks:

1. J. H. Silverman, The Arithmetic of Elliptic Curves.

p-adic Numbers, p-adic Analysis, and Zeta-Functions: p-adic numbers, p-adic interpolation of Riemann's zeta function, p-adic power series, rationality.

Textbooks:

1. 1. N. Koblitz, p-adic Numbers, p-adic Analysis, and Zeta-Functions, Second edition.

Introduction to Iwasawa Theory: Cyclotomic fields, local units, Iwasawa algebras, and p-adic measures, cyclotomic unites, Euler system, Main conjecture.

Textbooks:

1. J. Coates and R. Sujatha, Cyclotomic Fields and Zeta Values.
2. L. C. Washington, Introduction to Cyclotomic Fields.

Function Field Arithmetic: Number fields and Function fields, Drinfeld modules, Explicit class field theory of Drinfeld modules, Gamma functions, Zeta functions.

Textbooks:

1. 1. D. S. Thakur, Function Field Arithmetic.

Introduction to p-adic Galois Representations:

Absolute Galois groups of non-archimedean local fields, classification of p-adic Galois representations in terms of certain objects from semi-linear algebra, the so-called étale \varphi - and (\varphi, \Gamma)-modules.

Textbooks:

1. J.-M. Fontaine and Y. Ouyang, Theory of p-adic Galois Representations, preprint.
2. L. Berger, An introduction to the theory of p-adic representations.