Fachbereich Mathematik und Statistik
Prof. Dr. Salma Kuhlmann
Dr. Lothar Sebastian Krapp
Michele Serra

Universität Konstanz

Pro-/Fachseminar on Number Theory – SoSe 2021

This is just a list of possible topics where you can find some ideas and references for preparing your presentations. Please feel free to search for other sources and/or to propose to us a completely different topic in Number Theory on which you would like to build your own seminar talk.

Main topics

1. **Survey Topics**
   (a) **Groundbreaking results in Number Theory and their proofs**
   See [1, p. 1–67].
   (b) **Applications of Number Theory to Cryptography**
   See [4, p. 105–174].
   (c) **Proof methods in Number Theory**
   See [8, p. 165–175].
2. **Number Fields**
   (a) **Cyclotomic fields**
   See [10, p. 596–605].
   (b) **Quadradric number fields**
   See [7, p. 65–77].
   (c) **Class number formula for quadratic number fields**
   See [15, p. 136–145].
3. **Elementary Number Theory**
   (a) **Properties of digits**
   See [19, p. 18–20].
   (b) **Periods of decimal expansions**
   See [19, p. 114–117].
   (c) **The sieve of Eratosthenes and primality tests**
   See [19, p. 20–21] and [4, p. 120].
   (d) **Perfect numbers**
   See [19, p. 29–32].
   (e) **Mersenne numbers**
   See [19, p. 32–33].
   (f) **Continued fractions**
   See [3, p. 43–61] and [7, p. 222–230].

Further topics

1. **Applications to public-key cryptography**
   (a) **Discrete logarithm problem, Diffie–Hellman and Elgamal cryptosystems**
   See [13, p. 64–73].
   (b) **Pohlig–Hellman Algorithm**
   See [13, p. 88–94].
   (c) **Factorisation of integers and RSA**
   See [13, p. 117–125].
   (d) **Quadratic reciprocity and Goldwasser–Micali Cryptosystem**
   See [13, p. 169–180].
   (e) **Cryptography and elliptic curves**
   See [3, p. 380–385].

2. **Analytic Number Theory**
   (a) **Distribution of prime numbers**
   See [6, p. 1–17].
   (b) **Arithmetic functions**
   See [6, p. 18–24].
   (c) **Dirichlet's theorem on arithmetic progressions**
   See [6, p. 35–44].
   (d) **Sums of two squares**
   See [6, p. 44–52].
   (e) **The gamma function**
   See [6, p. 53–58].
   (f) **Zeta functions**
   See [6, p. 58–66].

3. **Diophantine Geometry**
   (a) **Versions and applications of the Chinese Remainder Theorem**
   See [19, p. 57–64].
   (b) **Polynomial congruences**
   See [19, p. 66–70].
   (c) **Congruences modulo p^n**
   See [19, p. 77–79].
   (d) **Pell's Equation and its relation to $\mathbb{Q}(\sqrt{d})$**
   See [7, p. 185–196].
   (e) **Linear diophantine equations and congruences**
   See [18, p. 229–235] and [7, p. 27–35].
   (f) **Quadratic diophantine equations and congruences**
   See [18, p. 236–237].

More advanced topics

1. **Transcendental Number Theory**
   (a) **Transcendence bases**
   See [5, p. 291–298].
   (b) **Transcendence of π**
   See [2, p. 5–6].
   (c) **Transcendence of e**
   See [2, p. 3–4].
   (d) **Exponential polynomials**
   See [7, p. 265–267].
   (e) **Schanuel's Conjecture**
   See [16, p. 111–121].

2. **p-adic Numbers**
   (a) **Valuation Theory and the p-adic valuation**
   See [17, p. 3–6].
   (b) **The field of p-adic numbers**
   See [9, p. 64–68].

3. **Set Theory and Logic**
   (a) **Peano Arithmetic and the natural numbers**
   See [12, p. 52–65].
   (b) **Set theoretic constructions of $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$**
   See [11, Sections 2.2–2.4].
   (c) **Typographical Number Theory**
   See [14, p. 204–230].

References

[1] M. Aigner and G. M. Ziegler, *Das BUCH der Beweise*, 4th edn (Springer Spektrum, Berlin, 2015).

[2] A. Baker, *Transcendental Number Theory* (Cambridge University Press, Cambridge, 1975).

[3] M. W. Baldoni, C. Cilberto and G. M. Piacentini Cattaneo, *Elementary Number Theory, Cryptography and Codes* (Springer, Berlin, 2009).

[4] A. Beutelspacher, H. B. Neumann and T. Schwarzpaul, *Kryptografie in Theorie und Praxis: Mathematische Grundlagen für elektronisches Geld, Internetsicherheit und Mobilfunk* (Vieweg, Wiesbaden, 2005).

[5] S. Bosch, *Algebra*, 6th edn (Springer, Berlin, 2006).

[6] J. Brüdern, *Einführung in die analytische Zahlentheorie*, (Springer, Berlin, 1995).

[7] P. Bundschuh, *Einführung in die Zahlentheorie*, 6th edn (Springer, Berlin 2008).

[8] M. Carl, *Wie kommt man darauf?* (Springer, Wiesbaden, 2017).

[9] L. van den Dries, 'Lectures on the Model Theory of Valued Fields', *Model Theory in Algebra, Analysis and Arithmetic*, Lecture Notes in Mathematics 2111 (ed. D. Macpherson and C. Toffalori; Springer, Heidelberg, 2014) 55–157.

[10] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd edn (Wiley, New York, 2004).

[11] D. Goldrei, *Classic Set Theory: For guided independent study* (Chapman & Hall, London, 1996).

[12] D. W. Hoffmann, *Die Gödel'schen Unvollständigkeitssätze: Eine geführte Reise durch Kurt Gödels historischen Beweis*, (Springer Spektrum, Berlin, 2013).

[13] J. Hoffstein, J. Pipher and J. H. Silverman, *An introduction to mathematical cryptography* (Springer, New York, 2014).

[14] , D. R. Hofstadter, *Gödel, Escher, Bach: an Eternal Golden Braid*, anniversary edn (Basic Books, New York, 1999).

[15] D. A. Marcus, *Number Fields*, 2nd edn (Springer, Cham, 2018).

[16] M. R. Murty and P. Rath, *Transcendental Numbers* (Springer, New York, 2014).

[17] P. Ribenboim, *The Theory of Classical Valuations*, Springer Monographs in Mathematics (Springer, New York, 1999).

[18] H. Scheid and A. Frommer, *Zahlentheorie*, 4th edn (Elsevier, SAV, München, 2007).

[19] C. Vanden Eynden, *Number Theory: An Introduction to Proof* (International Textbook Company, Scranton, Pennsylvania, 1970).