Mathematisches Institut der Universität München
Sommersemester 2013

Lukas-Fabian Moser

Seminar zur Zahlentheorie – Vortragsplan

Die angegebenen Kapitel sind jeweils, wenn nicht anders angegeben, zur Vorbereitung *vollständig* durchzuarbeiten. Eine Auswahl des tatsächlich vorzutragenden (und für die schriftliche Ausarbeitung relevanten) Stoffes wird dann im Laufe der Vorbesprechungen getroffen.

1. Sitzung (19. April 2013): Einführung

2. Sitzung (26. April 2013): Liegt zwischen n und $2n$ stets eine Primzahl?

Die Formel von Legendre, Divergenz der Reihe $\sum_p \frac{\log p}{p}$, Satz von Čebyšëv, Bertrandsches Postulat.
Literatur: [SF, I.4] und [BB, Kapitel 2].

3. Sitzung (3. Mai 2013): Warum ist $n^2 - n + 41$ für $n = 1, \ldots, 40$ eine Primzahl?

Thema des Vortrages ist das Quadratische Reziprozitätsgesetz. Legendresymbole, Formulierung des Quadratischen Reziprozitätsgesetzes und zwei Beweise (nach Eisenstein und mit Gaußschen Summen). Beispiele und Anwendungen, insbesondere Polynome der Form $x^2 - x + p$.
Literatur: [BB, Kapitel 5] und [SF, V.3]

4. Sitzung (10. Mai 2013): Wie faktorisiert man große Zahlen?

Faktorisierungsverfahren, Mersennesche und Fermatsche Primzahlen, Carmichael-Zahlen, Rabin-Test, RSA- und Rabin-Verschlüsselung, stochastische Faktorisierungsverfahren. (Algorithmen brauchen nicht formal als Pseudocode angegeben zu werden.)
Literatur: [SF], Abschnitte I.3, III.8, III.9, IV.6

5. Sitzung (17. Mai 2013): Welche Zahlen sind Summe zweier Quadratzahlen?

Der Zwei-Quadrate-Satz und der Vier-Quadrate-Satz. Zu ersterem soll auf jeden Fall der Beweis von Heath-Brown behandelt werden, am besten auch in seiner Formulierung von Zagier. Beim Vier-Quadrate Satz soll der Zusammenhang mit Quaternionen hergestellt werden.
Literatur: [BB, Kapitel 4], [SF, V.5], [Z]. Die Quaternionen werden in vielen Büchern über Lineare Algebra oder Algebra behandelt.

6. Sitzung (24. Mai 2013): Welche ganzzahligen Lösungen hat die Gleichung $x^n + y^n = z^n$?

Pythagoräische Zahlentripel und die Fermatsche Vermutung. Bestimmung aller ganzzahligen Lösungen der Gleichung $x^n + y^n = z^n$ für $n = 2, 3, 4$. Beweis der Faktorialität des Rings $\mathbb{Z}[\frac{1+i\sqrt{3}}{2}]$ (wird für den Fall $n = 3$ benötigt). Einige Bemerkungen zur Geschichte der Fermatschen Vermutung.
Literatur: [SF, V.6]

7. Sitzung (31. Mai 2013): Gibt es endliche Schiefkörper?

Das Hauptthema dieser Sitzung ist die Theorie der Kreisteilungspolynome über $\mathbb{Q}$ (Definition und Ganzzahligkeit wie in [BB], Irreduzibilität beispielsweise nach Landau oder Levi, siehe auch [C, 9.1.9]). Als Anwendung der Kreisteilungspolynome soll der Satz von Wedderburn mit dem Beweis von Ernst Witt vorgestellt werden.
Literatur: [BB, Kapitel 6], [La], [Le].

8. Sitzung (7. Juni 2013): Kann man Würfel verdoppeln und Winkel dreiteilen?

Definition konstruierbarer komplexer Zahlen (etwa nach [C, Chapter 10] bis Example 10.1.11), Nachweis der Körpereigenschaft. Beweis des Satzes, daß $z \in \mathbb{C}$ genau dann konstruierbar ist, wenn eine Kette von Körpererweiterungen $Q = K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathbb{C}$ gibt mit $z \in K_n$ und $[K_i : K_{i-1}] = 2$ für alle i (Theorem 10.1.6 in [C]). Beweis der Konstruierbarkeit des Fünfecks und des Siebzehnecks (Skizze), Unmöglichkeit der Lösung des Delischen Problems. Außerdem: Der Körper der Origami-konstruierbaren Zahlen, Drittelung des Winkels (mit Beweis).
Literatur: [C], Chapter 10, darin: Abschnitt 10.1 ohne 10.1.12/10.1.13 sowie 10.3 ohne 10.3.6 bis 10.3.9. (aber mit Exercise 1)

9. Sitzung (14. Juni 2013): Kann man das regelmäßige Siebeneck konstruieren . . . oder falten?

Übersetzung der körpertheoretischen Konstruier- bzw. Faltbarkeitskriterien vom letzten Mal in eine Aussage über den Grad des Zerfällungskörpers des Minimalpolynoms. Dazu ist die benötigte Galois- und Gruppentheorie crashkursartig bereitzustellen, inklusive einiger exemplarischer Beweise. (Erwähnt werden sollten mindestens: Zerfällungskörper, Hauptsatz der Galoistheorie, Galoisscher Abschluß, Auflösbarkeit von p-Gruppen beweisen, Satz von Burnside nur zitieren. Es darf Charakteristik 0 vorausgesetzt werden, so daß Separabilitätsfragen unsichtbar werden.)
Literatur: Für die Galoistheorie diverse Algebrabücher, gut geeignet ist auch [C]. Für die Konstruierbarkeitsaussagen: [C], Chapter 10, darin 10.1.12 ff., 10.2 und 10.3.6 ff.

10. Sitzung (21. Juni 2013): Und was ist mit der Quadratur des Kreises?

Zunächst die Irrationalitätsbeweise für e (von Fourier, 1815) und π (von Niven, 1947). Danach die Beweise der Transzendenz von e und (unter Verwendung von Funktionentheorie) π von Hilbert (1893), evtl. nur als Skizzen.
Literatur: [BB, Beginn von Kapitel 7] für die Irrationalität von e, [N], [H]

11. Sitzung (28. Juni 2013): Warum hat die Oktave zwölf Halbtöne?

Eine Einführung in die Theorie der Kettenbrüche: Endliche und unendliche Kettenbrüche; periodische Kettenbrüche; Anwendungen von Kettenbrüchen auf Kalender, den Bau von Planetarien und Musiktheorie (Kettenbruchentwicklung von $\log_2 r$ für $r = \frac{3}{2}, \frac{4}{3}, \frac{5}{4}, \frac{6}{5}, \frac{9}{8}$). Approximierbarkeit reeller Zahlen durch rationale Zahlen und die Anwendung auf Transzendenzbeweise. Approximationssatz von Dirichlet ([SF, I.10 Satz 27], in Absprache mit den Vortragenden der 13. Sitzung, evtl. auch erst dort) Der Satz von Chinčin über die geometrischen Mittel der Einträge einer Kettenbruchentwicklung (höchstens mit Beweisskizze), der Satz von Chinčin-Lévy für die n-te Wurzel des Nenners des n-ten Näherungsbruchs (ohne Beweis). Numerisches Ausprobieren beider Sätze für Zahlen wie $e, \pi, \sqrt{2}$ usw. (etwa mit Maple).
Literatur: [SF], I.8 und I.9, [R], [RS], §9

12. Sitzung (5. Juli 2013): Wie zählt man surjektive Abbildungen?

Der Ring der Zahlentheoretische Funktionen, Dirichletprodukt, Cauchyprodukt, Binomialprodukt und weitere Produkte. Charaktere modulo m, ihre Anzahl, der Hauptcharakter, Orthogonalitätsrelationen.
Literatur: [SF], Abschnitte VI.1 (bis zu den Möbiusschen Umkehrformeln), VI.2, VI.3 (nur Begriff der Dirichletreihe, Produktformel und Beispiele 2 bis 5), VI. 5 sowie Aufgabe VI.7.29. Charaktere finden sich in Abschnitt VII.5, wobei die dortigen Hilfssätze 1 und 2 zu behandeln sind. Teil der Aufgabe ist es, den Fehler im Beweis von Hilfssatz 1 zu finden und zu korrigieren!

13. Sitzung (12. Juli 2013): Mehr über die Darstellung von Zahlen als Summe von Quadratzahlen

Sätze über die Anzahl der Darstellungen natürlicher Zahlen als Summe von zwei oder vier Quadratzahlen. Auch der Beweis des Approximationssatzes von Dirichlet ([SF, I.10 Satz 27]) gehört zum Stoff, sofern er nicht von den Vortragenden der 11. Sitzung übernommen wurde.
Literatur: [SF], Abschnitt VIII.4

14. Sitzung (19. Juli 2013): Wieviele abelsche Gruppen gegebener Größe gibt es?

Die Theorie der Partitionen nach [SF]: Erzeugende Funktionen, verschiedene vs. ungerade Summanden, Summanden $\leqslant m$ vs. $\leqslant m$ Summanden, Eulersche Reihe, Rekursionsformeln, Ramanujansche Teilbarkeitsbeziehungen, Größenordnung von $p(n)$. Der Zusammenhang von Partitionszahlen und Konjugationsklassen in S_n sowie der Zahl der Isomorphieklassen abelscher Gruppen gegebener Ordnung (vgl. Struktursatz über endlich erzeugte abelsche Gruppen).
Literatur: [SF], Abschnitt VIII.2

Literatur

[BB] Aigner/Ziegler, Das BUCH der Beweise, 3. Auflage, Springer

[C] Cox, Galois Theory, Second Edition, Wiley

[H] Hilbert, Über die Transcendenz der Zahlen e und π, Mathematische Annalen 43 (1893), 216–219

[La] Landau, Über die Irreduzibilität der Kreisteilungsgleichung, Mathematische Zeitschrift 29 (1929), 462

[Le] Levi, Zur Irreduzibilität der Kreisteilungspolynome, Compositio Mathematica 1 (1935), 303–304

[N] Niven, A simple proof that π is irrational, Bulletin of the American Mathematical Society 53 (1947), 509

[RS] Rockett/Szüsz, Continued Fractions, World Scientific

[R] Ryll–Nardzewski, On the ergodic theorems (II) (Ergodic theory of continued fractions), Studia Mathematica 12.1 (1951), 74–79.

[SF] Scheid/Frommer, Zahlentheorie, 4. Auflage, Spektrum Akademischer Verlag

[Z] Zagier, A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares, American Mathematical Monthly 97 (1990), 144