Tübingen, den 18. März 2014

Vorträge

1. **Primzahlen und Teilbarkeitstheorie** (Dennis Gebhart)
   Beweise für Unendlichkeit der Primzahlen, Fermatzahlen, Mersennesche Primzahlen, Teilbarkeit in Integritätsringen, euklidische Ringe, Hauptidealringe, faktorielle Ringe, Beispiel Gaußsche Zahlen, Primfaktorzerlegung
   Literatur: [MSJ] Kapitel 1 und 2, [Bu] Kapitel I,§1,§2 und §5

2. **Vollkommene Zahlen und Fibonacci-Folgen** (Corinna Karl)
   Vollkommene Zahlen, Fibonacci Folgen, Goldener Schnitt, Fomel von Moivre-Binet, Fibonacci-Zahlen in der Natur
   Literatur: [Pa] Kapitel IX, [PH] Kapitel 3

3. **Euklidischer Algorithmus und Kongruenzrechnung** (Aline Fuchs)
   ggT, euklidischer Algorithmus, erweiterter euklidischer Algorithmus, kgV, Kongruenzrechnung, kleiner Satz von Fermat, Lösbarkeit von linearen Kongruenzen, Chinesischer Restesatz
   Literatur: [MSJ] Kapitel 3 und 4, [Bu] Kapitel I,§2 und §3, Kapitel 2 §1 und §2

4. **Primzahlen und deren Anwendung in der Kryptographie** (Yvonne Huber)
   Euler'sche Phi-Funktion, Sätze von Fermat, Euler, Wilson und deren Bedeutung in der Kryptographie, Grundlagen Kryptographie, RSA-Verfahren
   Literatur: [Bu] Kapitel II 3.1-3.9, [MSJ] Kapitel 5, [B] Kapitel 9.3

5. **Struktur der Einheitengruppe und Primitivwurzeln** (Mustafa Kavak)
   Endlich erzeugte abelsche Gruppen, Primitivwurzeln modulo Primzahlen, zu welchen Moduln sind Primitivwurzeln möglich? Potenzreste
   Literatur: [Bu] Kapitel II 5.1-5.5/1.1-1.7, [MSJ] Kapitel 6 und 7

6. **Legendre-Symbol und quadratische Reziprozität** (Marina Gassner)
   Legendresymbol, Euler-Kriterium, Lemma von Gauß, quadratisches Reziprozitätsgesetz, Ergänzungssätze, Jacobi-Symbol
   Literatur: [Bu] Kapitel III 2.1.-2.7 (benötigt teilweise auch 1.1-1.7), [MSJ] Kapitel 8

7. **Quadratsummen** (Sina Herrmann)
   Summe zweier Quadrate, Lemma von Thue, Summe von vier Quadraten, Satz von Lagrange, Summe von drei Quadraten
   Literatur: [Bu] Kapitel IV 1.1.-1.6, [MSJ] Kapitel 9

8. **Diophantische Gleichungen** (Bastian Wade)
   Lineare diophantische Gleichungen, pythagoräische Tripel, Rationale Punkte auf Kurven, Fermats-Vermutung
   Literatur: [Bu] Kapitel IV 2.1-2.8, [MSJ] Kapitel 16

9. **Kettenbrüche** (Stefanie Layher)
   Kettenbrüche, Kettenbruchalgorithmus, Konvergenz der Kettenbruchentwicklung, Satz von Euler/Lagrange
   Literatur: [MSJ] Kapitel 10, [Bu] Kapitel V, §3

10. **Primzahltests** (Tabea Herrmann)
    Grundlegendes über Primzahltests, Lucas-Lehmer Test, Lucas Test, Pepin Test, Solovay-Strassen Test, Miller-Rabin Test
    Literatur: [MSJ] Kapitel 11

11. **Faktorisierungsalgorithmen** (Pirmin Glück)
    Primfaktorzerlegung, Faktorisierungsalgorithmen, Faktorbasis, Kettenbruchalgorithmus von Brillhart-Morrison, quadratisches Sieb, Überblick über weitere Algorithmen
    Literatur: [MSJ] Kapitel 12

Literatur

[AZ] Aigner M., Ziegler, G. M.: Buch der Beweise, Springer (2003).

[B] Buchmann, J.: Einführung in die Kryptographie, Springer (2010).

[Bu] Bundschuh, Peter: Einführung in die Zahlentheorie, Springer (1992).

[H] Hausen, J.: Lineare Algebra I/II, Shaker-Verlag.

[M] Matthes, R.: Algebra, Kryptologie und Kodierungstheorie, Carl-Hanser-Verlag (2003).

[MSJ] Müller-Stach, Stefan/Piontkowski, Jens: Elementare und algebraische Zahlentheorie, Vieweg (2006).

[Pa] Padberg, Friedhelm: Elementare Zahlentheorie, Spektrum (2001).

[PH] Pracht E., Heidenreich K.: Elementare Zahlentheorie, Schöningh (1978).

[RS] Reiss K., Schmieder G.: Basiswissen Zahlentheorie, Springer (2007).

[S] Stroth G.: Elementare Algebra und Zahlentheorie, Springer (2012).