Programm des Seminar über Zahlentheorie
Wintersemester 2010/11

Vortrag 1: K. Kielemoniuk. Vollständige Induktion.

Literatur: [BRK], Kap. 1.

Vortrag 2: J. Schwarz. Euklidischer Algorithmus und Stellenwertsysteme.

Literatur: [BRK], Kap. 2.1 und 2.2

Vortrag 3: I. Heine. Gruppen und Ringe.

Literatur: [BRK], Kap. 2.5

Vortrag 4: V. Wall. Primzahlen.

Literatur: [BRK], Kap. 2.7

Vortrag 5: S. Numrich. Chinesischer Restsatz und Euler-Funktion.

Literatur: [BRK], Kap. 2.8 und 2.9

Vortrag 6: J. Quaß. Kleiner Fermat und Primitivwurzeln.

Literatur: [BRK], Kap. 3.1 – 3.3

Vortrag 7: M. Wehry. Quadratische Reste

Literatur: [BRK], Kap. 3.4

Vortrag 8: S. Lunde. Polynome.

Literatur: [RW], Kap. 3.4

Vorträge 9 und 10: S. Karata und F. Sarikaya. Kryptographie und RSA.

Literatur: [BRK], Kap. 2.6, [RW], Kap. 4.1 und 4.2 und weitere Literatur

Vortrag 11: Primzahlverteilung (J. Frenser).

Literatur: [RW], Kap. 4.3 – 4.5

Vortrag 12: S. Küttner. AKS-Algorithmus, Teil 1.

Literatur: [RW], Kap. 5

Vortrag 13: M. Heckner. AKS-Algorithmus, Teil 2.

Literatur: [RW], Kap. 6

Vortrag 14: R. Kahlmeier. AKS-Algorithmus, Teil 3.

Literatur: [RW], Kap. 7

Vortrag 15: W. Stach. Der Satz von Fermat für $n = 3$

Literatur: ...

Vortrag 16: S. Didouh. Der Satz von Fermat für $n = 4$

Literatur: ...

Vortrag 17: B. Agko. Summe von Quadraten

Literatur: [Me], Kap. 5.4

References

[BRK] Andreas Bartholomé, Josef Rung und Hans Kern, *Zahlentheorie für Einsteiger*, Vieweg Verlag. Online erhältlich unter
http://dx.doi.org/10.1007/978-3-8348-9650-6

[Me] H. Menzer, *Zahlentheorie*, Oldenbourg Verlag

[RW] Lasse Rampe und Rebecca Waldecker, *Primzahltests für Einsteiger*, Vieweg Verlag. Online erhältlich unter
http://dx.doi.org/10.1007/978-3-8348-9597-4