Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

Institut für
MATHEMATIK

Prof. Dr. Jörn Steuding · Julius-Maximilians-Universität
Institut für Mathematik · Emil-Fischer-Str. 40 · 97074 Würzburg

Prof. Dr. Jörn Steuding
Professur am Lehrstuhl Mathematik IV
(Zahlentheorie)

Institut für Mathematik
Emil-Fischer-Str. 40 · Zimmer 02.012
Telefon: 0931/31-85008
Sekretariat: 0931/31-85006
Telefax: 0931/31-85376

steuding@mathematik.uni-wuerzburg.de
www.mathematik.uni-wuerzburg.de/∼steuding

Würzburg, Wintersemester 2015/16

Oberseminar ZAHLENTHEORIE

Im Wintersemester 2015/16 findet regelmäßig ein Oberseminar Zahlentheorie statt, jeweils **montags um 16:15 Uhr im SE40**. Die Vorträge im Kalenderjahr 2015 sind:

- 5. Oktober: Jörn Steuding (Wü): Open Conjectures in Zeta-Function Theory I
- 12. Oktober: Jörn Steuding (Wü): Open Conjectures in Zeta-Function Theory II
- 19. Oktober: Jörn Steuding (Wü): Open Conjectures in Zeta-Function Theory III
- 16. November: Marc Technau (Wü): Special Values in Beatty Sequences
- 23. November: Karin Halupczok (Münster): Polynomial large sieve inequalities and a Bombieri–Vinogradov theorem with products of Gaussian primes
- 30. November: Thomas Lachmann (Wü): Euclidean Proofs in Function Fields
- 7. Dezember: Florian Göpfert (Darmstadt): Lattice based cryptography

Interessierte Zuhörer sind herzlichst willkommen! Einige Abstracts zu den Vorträgen befinden sich auf der nächsten Seite.

Mit freundlichen Grüßen,

Jörn Steuding.

Jörn Steuding (Wü): Open Conjectures in Zeta-Function Theory

We give a concise introduction to the Riemann zeta-function and its relatives and highlight the main open problems concerning their value-distribution (with respect to denseness properties, the phenomenon of universality and questions around the distribution of complex zeros).

Marc Technau (Wü): Special Values in Beatty Sequences

We discuss questions about the occurrence of special values, e.g. primes, in Beatty sequences $\mathcal{B}(\alpha) = \{\lfloor n\alpha \rfloor \mid n \in \mathbb{N}\}$ ($\alpha > 0$ irrational). This is joint work with Jörn Steuding.

Karin Halupczok (Münster): Polynomial large sieve inequalities and a Bombieri–Vinogradov theorem with products of Gaussian primes

Polynomial versions of the large sieve inequality are presented. They contain advantages coming from ingredients of the work of S.T. Parsell, S.M. Prendiville and T.D. Wooley on mean value estimates for multidimensional Weyl sums. Some advantages and disadvantages of the Polynomial LSI compared to standard approaches are discussed. As an application, a variant of Bombieri–Vinogradov's Theorem with appropriate products of Gaussian primes as moduli can be derived by adapting Vaughan's classical approach.

Thomas Lachmann (Wü): Euclidean Proofs in Function Fields

Schur proved the infinitude of primes in certain arithmetic progressions with non-analytic methods. We discuss an analogous proof for the primes in the ring $\mathbb{F}_q[Y]$.

Florian Göpfert (Darmstadt): Lattice based cryptography

The hardness of literally every cryptographic scheme used in practice today is based on number theoretical problems like factoring or discrete logarithm. However, since the groundbreaking work of Peter Shor it is known that those problems can be solved efficiently by quantum computers. Consequently, we need solutions that are based on problems that are believed remain hard even in the presence of those new computational environments. One of the most promising candidates for this is lattice-based cryptography. This talk gives a short glimpse into the field, introducing the underlying problems as well as the ideas and techniques used to construct the schemes.