

Institut für Mathematik,  
FG Kombinatorik/Graphentheorie  
Prof. Dr. Michael Stiebitz

## Vorlesungsankündigung

für das Wintersemester 2020/21



# Zahlentheorie

Die Zahlentheorie ist ein Teilgebiet der Mathematik, das sich mit den Eigenschaften der ganzen Zahlen beschäftigt. Die systematische Entwicklung der Zahlentheorie begann im ersten Jahrtausend v. Chr. im antiken Griechenland. Die beiden zentralen Probleme der Zahlentheorie sind das *Primzahlproblem* und das *Faktorisierungsproblem*. Beim Primzahlproblem geht es darum von einer natürlichen Zahl zu entscheiden, ob sie eine Primzahl ist. Beim Faktorisierungsproblem möchte man eine natürliche Zahl als Produkt zweier kleinerer Zahlen darstellen. Dies ist natürlich nur dann möglich, wenn die natürliche Zahl keine Primzahl ist. Beide Probleme scheinen eng zusammenzuhängen. Für die moderne Kryptographie ist es aber von entscheidender Bedeutung, dass der Schwierigkeitsgrad der beiden Probleme unterschiedlich ist. Im Jahre 2012 bewiesen Agrawal, Kayal und Saxena, dass das Primzahlproblem in Polynomialzeit lösbar ist. Ziel der Vorlesung Zahlentheorie ist es einen Beweis für diesen fundamentalen Satz zu geben.



## Vorlesungsinhalt

- Einführung
- Primzahlen
- Algebraische Hilfsmittel
- Primzahltest in Polynomialzeit
- Probabilistische Primzahltests

Vorlesung siehe Vorlesungsverzeichnis,  
Übung nach Vereinbarung