



# EINLADUNG

zu einem  
**VORTRAG**  
zum Thema

## "Wie man die Teiler großer Zahlen findet"

Markus Hittmeir, Dr. rer. nat

Department of Mathematics  
University of Salzburg

**Abstract:** Die Teilbarkeitsbeziehung zwischen natürlichen Zahlen ergibt sich direkt aus den Grundrechnungsarten und ist einfach zu verstehen. Jeder von uns kennt die Teiler von 15, 21 und 35 seit der Volksschule. Gleichzeitig ist diese Beziehung der wichtigste Forschungsgegenstand der elementaren Zahlentheorie und wirft schwierige Fragen über die Primzahlen auf. Kann jede gerade Zahl außer 2 als Summe von zwei Primzahlen geschrieben werden? Gibt es unendlich viele Primzahlzwillinge, also Paare von Primzahlen, deren Differenz gleich 2 ist? Diese und ähnliche Probleme sind seit Jahrhunderten ungelöst. Ein ebenso altes Problem, das in den letzten Jahrzehnten durch die Entwicklung von Computern eine Renaissance erlebt hat, beschäftigt sich mit der Berechnung der Teiler natürlicher Zahlen. Dieses sogenannte Faktorisierungsproblem ist für relativ kleine Zahlen einfach zu bewältigen. Für große Zahlen mit 500 Ziffern oder mehr ist es unter gewissen Voraussetzungen aber praktisch unlösbar. Das heißt, dass die derzeit besten Faktorisierungsverfahren auf den schnellsten Computern der Welt Jahrhunderte brauchen würden, um solche Zahlen in ihre Teiler zu zerlegen. Verschlüsselungsverfahren wie das nach seinen Erfindern benannte RSA nutzen diese Schwierigkeit aus. Die Sicherheit von E-Banking und Onlinetransaktionen ist davon abhängig, dass niemand in der Lage ist, die Teiler großer Zahlen zu finden.

In diesem Vortrag werden wir über das Faktorisierungsproblem, über Faktorisierungsverfahren und damit zusammenhängende Ideen aus meiner Dissertation sprechen.

**Mittwoch, 15.05.2019, 13:45 Uhr s.t.**

Laborgebäude Itzling (Science City), HS Christian Doppler,  
Jakob Haringerstr. 2a, 5020 Salzburg



gez. Fachbereichsleiter Univ.-Prof. Dr. Fritz Aberger  
gez. Fachbereichsleiter Univ.-Prof. Dr. Hans Brandstetter  
*Fachbereich Biowissenschaften*