

Modulbezeichnung		Kurzbezeichnung
Algorithmic Number Theory		10-M=VAZTin-211-mo1
Modulverantwortung		anbietende Einrichtung
Studiendekan/-in Mathematik		Institut für Mathematik
ECTS	Bewertungsart	zuvor bestandene Module
10	numerische Notenvergabe	--
Moduldauer	Niveau	weitere Voraussetzungen
1 Semester	weiterführend	--
Inhalte		
Binärzahlen, Berechnung des größten gemeinsamen Teilers, Pseudoprimitivzahltests, Berechnung von Primitivwurzeln, Primzahltests für Fermat- und Mersenne-Zahlen, Faktorisierungsverfahren (Pollard-Rho, $(p-1)$ -Verfahren, elliptische Kurvenmethode, quadratisches Sieb), diskreter Logarithmus		
Qualifikationsziele / Kompetenzen		
Die/Der Studierende kennt die theoretischen Grundlagen und die Anwendungsmöglichkeiten verschiedener Methoden der algorithmischen Zahlentheorie.		
Lehrveranstaltungen (Art, SWS, Sprache sofern nicht Deutsch)		
V (4) + Ü (2) Veranstaltungssprache: Englisch		
Erfolgsüberprüfung (Art, Umfang, Sprache sofern nicht Deutsch / Turnus sofern nicht semesterweise / Bonusfähigkeit sofern möglich)		
a) Klausur (Regelfall) (ca. 90-120 Min.) oder b) Mündliche Einzelprüfung (ca. 20 Min.) oder c) Mündliche Gruppenprüfung (2 TN, je ca. 15 Min.) Prüfungssprache: Englisch Prüfungsturnus: Im Semester der LV und im Folgesemester Bonusfähig		
Platzvergabe		
--		
weitere Angaben		
--		
Arbeitsaufwand		
300 h		
Lehrturnus		
k. A.		
Bezug zur LPO I		
--		
Verwendung des Moduls in Studienfächern		
Master (1 Hauptfach) Mathematics International (2021) Master (1 Hauptfach) Mathematics International (2022)		