

INHALTsverzeichnis der Vorlesung Einführung in die Zahlentheorie

WiSe '26/'27, hhu
K. Halupczok

ez 1: Teilbarkeit

Teiler, Vielfache, Gegenteiler, Gaußklammer, Division mit Rest, kleinster nichtnegativer und absolut kleinster Rest, ggT, teilerfremd, Satz von Bézout, AgV

ez 2: Hauptsatz der Arithmetik

Primzahl, Unendlichkeit der Primzahlenfolge, Sieb des Eratosthenes, Lemma von Euklid, Satz von der eindeutigen PFZ/Hauptsatz der Arithmetik, Primfaktorzerlegung, PFZ des ggT und kgV

ez 3: Euklidischer Algorithmus

Bézout-Identität, Euklidischer Algorithmus, explizite ggT-Berechnung und Berechnung der Bézout-Koeffizienten, lineare diophantische Gleichung, endlicher Kettenbruch

ez 4: Kettenbrüche

Endlicher Kettenbruch, Teilnenner, Kettenbruchentwicklung (KBE), Näherungsbruch (NB), Rekursionsformeln für NB, normierter KB, erweiterter euklidischer Algorithmus = Schema zur Berechnung der Bézout-Koeffizienten

ez 5: Fibonaccizahlen

Fibonaccizahlen, KBE und Fibonaccizahlen, goldener Schnitt, Binetsche Formel, Formeln mit Fibonaccizahlen, Fibonacci-Primzahlen, Dauer des euklidischen Algorithmus (Satz von Lamé)

ez 6: Kongruenzrechnung

Kongruenz, modulo, Restklassen, inverse Restklasse, reduzierte Restklasse, Restklassensysteme, Lineare Kongruenz, Restklassenring, Chinesischer Restsatz, g-adische Darstellung / Ziffersysteme, Teilbarkeitsregeln

ez 7: Modulare Potenzen

Potenzrechnung mod m , schnelles Potenzieren, Satz von Euler (-Fermat) / Eulerkongruenz, Kleiner Satz von Fermat / Fermatkongruenz, Eulersche φ -Funktion, Ordnung

ez 8: Polynomielle Kongruenzen (mit beliebigen Modulen)

Lösungszahl, Multiplikativität der Lösungszahl laut CRS, Satz von Lagrange, Satz von Wilson, Aufsteigesatz (Hensels Lemma)

ez 9: Primitivwurzeln

Primitivwurzel, Satz von Euler über PWN , Konstruktion und Anzahl von PWN , binomische Kongruenzen, diskreter Logarithmus bzw. Index

ez 10: Quadratische Reste und das QRG

Quadratische und reinquadratische Kongruenz, qR und qNR , Eulerkriterium, Legendresymbol, Gaußsches Lemma, QRG, 1. EG, 2. EG

ez 11: Modulares Wurzelziehen und das Jacobisymbol

explizite Bestimmung der Lösungen von $x^2 \equiv a \pmod{p}$, Rechnen in $\mathbb{F}_{p^2}$ über $\mathbb{F}_p$, Jacobisymbol als Fortsetzung des Legendresymbols, QRG und EG für das Jacobisymbol, schnelle Berechnung des Jacobisymbols

ez 12: Algorithmische Zahlentheorie

Faktorisierungsproblem, RSA, Münzwurf am Telefon, DL-Problem, Diffie-Hellman, DH-Problem, El Gamal, Primzahltestproblem, Carmichaelzahl, Korselt-Kriterium, Miller-Rabin-Test

ez 13: Summen von Quadraten

Pythagoras, Summe von 2 Quad. und $\mathbb{Z}[i]$, 3-Quadratesatz von Legendre, 4-Quadrate-Satz von Lagrange, andere quadratische Formen und pythagoräische Quadrupel

ez 14: Höhere Potenzgleichungen

Fermatproblem, Fall $n=4$, abc-Vermutung, Fermat/Catalan für große Exponente, gemischte diophantische Gleichungen, Taxizahlen, Waring'sches Problem, Hardy/Littlewood

ez 15: Fermat- und Mersenne-Primzahlen

Fermatzahlen, regelmäßige n -Ecke, Pepins Test, Mersennezahlen, Sophie-Germain-Paare, Lucas-Test, Wieferich-Pz, vollkommene Zahlen

ez 16: Elementare Primzahltheorie

Primzahlzählfunktion $\pi(x)$, Satz von Tschebyschev, Primzahlsatz, logarithmisches Integral $\text{li}(x)$, Approximation von $\text{li}(x)$, Fehlerterm bei $\pi(x) \sim \text{li}(x)$, Riemannsche Vermutung (RH), Bertrands Postulat

Ende der Vorlesung