Übungen zur Vorlesung Angewandte Diskrete Mathematik

Institut für Reine Mathematik WS 08/09

Vorbereitung zur Probeklausur/Klausur

- Wie lauten die elementaren Teilbarkeitsregeln für 2 , 3 , 5 , 9 und 11 ?
- Eindeutigkeit der Primfaktorzerlegung
- Wie berechnet man ggT und kgV anhand der Primfaktorzerlegung?
- Wie funktioniert der erweiterte Euklidische Algorithmus?
- Wie rechnet man modulo?
- Wie berechnet man das multiplikative Inverse von a modulo n ?
- Wann existiert das multiplikative Inverse?
- Was ist die Eulersche φ -Funktion? Wie berechnet man diese?
- Wie berechnet man große Potenzen modulo n ?
- Was besagt der kleine Satz von Fermat?
- Was besagt der Satz von Euler?
- Wie funktioniert der schnelle Potenzier-Algorithmus?
- Was besagt der Chinesische Restsatz? Wie wendet man ihn an?
- Was ist der Exponent von a modulo n ? Wie bestimmt man ihn?
- Wie hängt der Exponent mit $\varphi(n)$ zusammen?
- Was ist eine Primitivwurzel?
- Für welche Zahlen n existiert eine Primitivwurzel modulo n ?
- Wie berechnet man eine Quadratwurzel aus a modulo p , falls $p \equiv 3 \mod 4$?
- Wie berechnet man eine Quadratwurzel aus a modulo n , falls n zusammengesetzt ist?
- Was ist eine Carmichael-Zahl?
- Wie kann man Carmichael-Zahlen charakterisieren?
- Wie funktioniert der Primzahltest von Rabin?
- Wie arbeitet die RSA-Verschlüsselung?
- Erweiterter Euklidischer Algorithmus für Polynome über $\mathbb{Q}$ bzw. über $\mathbb{Z}/p\mathbb{Z}$
- Wann ist ein Polynom irreduzibel (speziell für Grad 2/3)?
- Wie rechnet man in Körpern $\mathbb{Q}(\alpha)$?

- Wie berechnet man das Inverse zu einem gegebenen Element in $\mathbb{Q}(\zeta)$?
- Wie berechnet man das Produkt zweier Elemente in $\mathbb{Q}(\zeta)$?
- Wie rechnet man in endlichen Körpern $\mathbb{F}_q$?
- Wie berechnet man das Inverse zu einem gegebenen Element in $\mathbb{F}_q$?
- Wie berechnet man das Produkt zweier Elemente in $\mathbb{F}_q$?
- Was sind die Zech-Logarithmen? Wie rechnet man damit?
- Was ist die Spur von $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$?
- Wie berechnet man die Spur?
- Was ist die duale Basis zu einer Basis $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ von $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$?