Primzahltests und kryptographische Verfahren

Mathe-AG Workshop 3 - Ausblick

Romana Quaresma Martins, Fabio Wille, Peter Parczewski

10. November 2026



Teil I Primzahlen und Primzahltests

Primzahlen und mathematische Grundlagen

Primzahlen, Primfaktorzerlegung, Kleiner Satz von Fermat.

Primahltests

- Sieb des Eratosthenes
- Fermat-Primzahltest
- Miller-Rabin-Primzahltest (probabilistische Verfahren)

Mit solchen Problemen beschäftigen wir uns:

- **Primzahl oder zusammengesetzte Zahl?**
  Wie lässt sich möglichst effizient überprüfen, ob eine vorgegebene Zahl eine Primzahl ist? Muss man tatsächlich alle kleineren Zahlen als mögliche Teiler überprüfen?

Teil I Primzahlen und Primzahltests

- **Effiziente Primzahlsuche:** Wie lassen sich alle Primzahlen bis 100 oder 1000 möglichst systematisch bestimmen? Welche Vorteile bietet das Sieb des Eratosthenes gegenüber der Probedivision?
- **Grenzen von Primzahltests:** Kann ein Verfahren eine zusammengesetzte Zahl fälschlicherweise als Primzahl einstufen? Untersuchung des Fermat-Tests anhand von Pseudoprimzahlen, beispielsweise der Zahl 341.
- **Zuverlässigkeit und Effizienz:** Wie unterscheiden sich deterministische und probabilistische Primzahltests? Warum ist es sinnvoll, den Miller-Rabin-Test mehrfach mit unterschiedlichen Basen durchzuführen?
- **Große Primzahlen:** Wie kann man feststellen, ob sehr große Zahlen Primzahlen sind, wenn eine vollständige Überprüfung aller möglichen Teiler praktisch nicht mehr durchführbar ist?

Teil II Kryptgraphische Verfahren

Mathematische Grundlagen

Verschlüsselung und Entschlüsselung. Symmetrische und asymmetrische Verfahren. Modulare Arithmetik und Kongruenzen. **RSA-Verfahren**. Eulersche Φ-Funktion und Primfaktorzerlegung.

Mögliche Problemstellungen:

- **Geheime Nachrichten:** Wie können zwei Personen Nachrichten austauschen, ohne vorher einen gemeinsamen geheimen Schlüssel vereinbart zu haben? Welche Unterschiede bestehen zwischen symmetrischer und asymmetrischer Verschlüsselung?

Teil II Kryptgraphische Verfahren

- **RSA selbst anwenden:** Wie lässt sich aus zwei Primzahlen ein öffentlicher und ein privater Schlüssel konstruieren? Die Kinder könnten anhand kleiner Zahlen ein eigenes RSA-System erstellen und eine Nachricht verschlüsseln und entschlüsseln.
- **RSA knacken:** Ist es möglich, aus einem öffentlichen Schlüssel den privaten Schlüssel zu bestimmen? Untersuchung anhand kleiner RSA-Beispiele durch Primfaktorzerlegung.
- **Sicherheit großer Primzahlen:** Warum werden bei RSA große Primzahlen verwendet? Welche Rolle spielt die Schwierigkeit der Primfaktorzerlegung für die Sicherheit des Verfahrens?
- **Zusammenhang der beiden Themenbereiche:** Warum benötigt man zur Erstellung eines RSA-Schlüssels große Primzahlen, während die Primzahltests selbst wiederum andere mathematische Verfahren erfordern?