Diskrete Mathematik **FTB-INF**
Dr. Martin E. Müller, Simon Fetzel **WS 24/25**

Übungsblatt 4 - Primzahlen, RSA-Kryptosystem

1. Modifizieren Sie die Funktion `isPrime` aus der Vorlesung in der Art, dass *nur* jeweils bis zu $\sqrt{n}$ auf Teilbarkeit geprüft wird. Skizzieren Sie den Beweis aus der Vorlesung in eigenen Worten.

2. Was besagt der Fundamentalsatz der Arithmetik?

3. Berechnen Sie die kanonische Primfaktorzerlegung für ein paar fünfstellige Zahlen Ihrer Wahl. Prüfen Sie Ihre Resultate mit der Funktion `primeFactors(n)` aus der Vorlesung und versuchen Sie auch, diese zu verstehen.

4. Geben Sie den Wert der Variable `result` der Methode `pzSieb(n)` aus der Vorlesung bei Aufruf mit $n = 97$ nach den ersten drei Iterationen an.

5. Geben Sie mindestens einen Grund an, warum die Funktion `pzSieb(n)` aus der Vorlesung unbrauchbar für einen Primzahltest (ist eine Zahl prim oder nicht?) von großen Zahlen (100 Dezimalstellen und mehr) ist. Warum dürfen wir die Schleife beenden, sobald $c^2 \geq n$ ist?

6. Erweitern Sie die PYTHON-Funktion `caesarEnc(msg, key)` aus der Vorlesung derart, dass Nachrichten mit Klein- und Großbuchstaben verschlüsselt werden können.

7. Schreiben Sie eine PYTHON-Funktion `caesarDec(msg, key)` welche eine mit der Cäsar-Verschlüsselung verschüsselte Nachricht entschlüsselt und zurückgibt.

8. Implementieren Sie das in der Vorlesung vorgestellt RSA-Kryptosystem nach und ver- und entschlüsseln Sie einige Nachrichten damit. Verwenden Sie dazu andere Primzahlen p und q wie in der Vorlesung.
   Was ist die größte Nachricht (Zahl) die Sie damit verschlüsseln können?
   Warum wäre es einfach eine Nachricht ohne d zu entschlüsseln, wenn man p und q hat?

Theoriefragen:

1. Was ist eine Primzahl?
2. Was ist (informell) ein Ring?
3. Was ist das Sieb des Eratosthenes?
4. Wie funktioniert das RSA-Kryptosystem?
5. Was besagt der Fundamentalsatz der Arithmetik?