Aufgaben zu Kapitel 5: Primzahl-Tests

Aufgabe 5.1 (Grosse Primzahlen 1) Für das RSA-Verfahren und andere Kryptosysteme werden sehr große Primzahlen benötigt.

a) Gibt es überhaupt beliebig große Primzahlen? Begründen Sie Ihre Antwort.

b) Wie kann man die Anzahl der Primzahlen einer bestimmten Größenordnung abschätzen?

c) Wieviel Prozent siebenstelliger Dezimalzahlen sind vermutlich Primzahlen?

Aufgabe 5.2 (Grosse Primzahlen 2) Erläutern Sie kurz, wie man geeignet große Primzahlen findet. Nennen Sie dabei die verwendeten Verfahren. Warum verwendet man keine deterministischen Verfahren, um Primzahlen zu bestimmen?

Aufgabe 5.3 (Fermat-Test)

a) Beschreiben Sie den Ablauf eines Fermat-Tests.

b) Was versteht man unter einer (fermatschen) Pseudoprimzahl?

c) Was versteht man unter einer Carmichael-Zahl?

d) Prüfen Sie mithilfe des Fermat-Tests, ob 161 eine Primzahl ist. Wählen Sie als Basis $a = 5$.

Aufgabe 5.4 (Miller-Rabin-Test)

a) Beschreiben Sie den Ablauf eines Miller-Rabin-Tests.

b) Was versteht man unter einer starken Pseudoprimzahl?

c) Prüfen Sie mithilfe des Miller-Rabin-Test, ob 217 eine Primzahl ist. Wählen Sie als Basis $a = 2$. Was wissen Sie nach dem Test über die Zahl 217?

d) Prüfen Sie mithilfe des Miller-Rabin-Test, ob 703 eine Primzahl ist. Wählen Sie als Basis $a = 3$. Was wissen Sie nach dem Test über die Zahl 703?