Aufgaben zu Kapitel 5: Primzahl-Tests

Aufgabe 5.1 (Grosse Primzahlen 1)

a) Ja, es gibt unendlich viele Primzahlen (Satz von Euklid).

b) Der Primzahlsatz besagt, dass es etwa $n/\ln(n)$ Primzahlen kleiner oder gleich n gibt. Die Differenz des Funktionswerts an der oberen Grenze des Bereichs minus dem Funktionswert an der unteren Grenze ist eine Abschätzung der Anzahl der Primzahlen im interessierenden Bereich.

c) Anzahl siebenstelliger Primzahlen ist ungefähr

$$9999999/\ln(9999999) - 999999/\ln(999999) \approx 620420,63 - 72382,35 \approx 548038,28.$$

Prozentualer Anteil: 6,09 %.

Aufgabe 5.2 (Grosse Primzahlen 2) Es wird eine ungerade Zahl n der gewünschten Größenordnung gewählt. Diese wird mit unterschiedlichen Basen und den Tests von Fermat oder besser Miller-Rabin untersucht. Werden alle Tests bestanden und war die Anzahl der verwendeten Basen groß, ist die Zahl mit hoher Wahrscheinlichkeit eine Primzahl. Wird auch nur ein Test nicht bestanden, ist die Zahl sicher keine Primzahl und es wird ein neuer Primzahlkandidat (z. B. $n+2$) untersucht. Dies wird wiederholt, bis eine Zahl gefunden wird, die die Tests besteht.

Deterministische Primzahltestverfahren verursachen einen so hohen Aufwand, dass sie bei sehr großen Zahlen in der Praxis viel zu viel Zeit in Anspruch nehmen würden.

Aufgabe 5.3 (Fermat-Test)

a) Siehe Folie 57.

b) Eine fermatsche Pseudoprimzahl ist eine zusammengesetzte Zahl n, für die es eine Basis a gibt mit $a^{n-1} \mod n = 1$.

c) Eine Carmichael-Zahl ist eine zusammengesetzte Zahl, die eine Pseudoprimzahl für alle Basen $\{2, \ldots, n-1\} \backslash \{\text{Teilern von } n\}$ ist.

d) $\text{ggT}(161, 5) = 1$;

$$a^{n-1} \mod n = 5^{160} \mod 161 = (5^{128} \cdot 5^{32}) \mod 161 = (32 \cdot 144) \mod 161 = 100 \neq 1.$$

Somit ist 161 sicher keine Primzahl.

Aufgabe 5.4 (Miller-Rabin-Test)

a) Siehe Folie 59.

b) Eine starke Pseudoprimzahl ist eine zusammengesetzte Zahl, die für bestimmte Basen a den Miller-Rabin-Test besteht.

c) $n - 1 = 216 = 27 \cdot 2^3$;

$$2^{1 \cdot 27} \mod 217 = 190;\ 2^{2 \cdot 27} \mod 217 = 78;\ 2^{4 \cdot 27} \mod 217 = 8;\ 2^{8 \cdot 27} = 64.$$

$(190, 78, 8, 64)$ ist eine ungültige Folge. Somit ist 217 sicher keine Primzahl.

d) $n - 1 = 702 = 351 \cdot 2^1$;

$$3^{1 \cdot 351} \mod 703 = 702;\ 3^{2 \cdot 351} \mod 703 = 1.$$

$(702, 1)$ ist eine gültige Folge. Somit ist der Test bestanden. 703 ist daher mindestens mit der Wahrscheinlichkeit 3/4 eine Primzahl.