

Carmichaelzahlen und Pseudoprimzahlen

1. Carmichaelzahlen

Erstellen Sie eine Prozedur *isCarmichael*, die eine Zahl testet, ob sie eine Carmichaelzahl ist.

Definition: Sei $n \in \mathbb{N}$ eine zusammengesetzte Zahl.

Gilt für alle $a \in \mathbb{N}$ mit $\text{ggT}(a, n) = 1$: $a^{n-1} \equiv 1 \pmod{n}$, so heißt n Carmichaelzahl.

Hinweise: Es reicht, alle Zahlen $a \in \mathbb{N}$ mit $1 < a < n$ und $\text{ggT}(a, n) = 1$ zu testen.

Eingabe: positive Zahl n

Ausgabe: n Carmichaelzahl \Rightarrow **TRUE**; n keine Carmichaelzahl \Rightarrow **FALSE**

im Detail: 1. Ist n eine Primzahl, dann ist n keine Carmichaelzahl. (Nutzen Sie *isprime(n)*.)

2. Teste alle Zahlen a von 2 bis $n - 1$:

Wenn $\text{ggT}(a, n) = 1$ und $a^{n-1} \not\equiv 1 \pmod{n}$, dann ist n keine Carmichaelzahl.

(Nutzen Sie **igcd(a, n)** und **a^(n-1) mod n**.)

3. Da nun alle Bedingungen der Definition erfüllt sind, ist n eine Carmichaelzahl.

Fragen: 1. Welche der Zahlen sind Carmichaelzahlen? 341, 401, 561, 1009, 1011, 1105, 1729, 2465

Die Zahlen _____ sind Carmichaelzahlen.

2. Was fällt Ihnen bei dem Test bezüglich der Rechenzeiten auf?

Wann dauert der Test lange? Warum?

2. Pseudoprimzahlen zu einer vorgegebenen Basis a

Erstellen Sie eine Prozedur *isPseudoprime*, die eine Zahl testet, ob sie Pseudoprimzahl zur Basis a ist.

Definition: Sei n eine ungerade zusammengesetzte Zahl.

Gibt es ein $a \in \mathbb{N}$ mit $a^{n-1} \equiv 1 \pmod{n}$, so heißt n Pseudoprimzahl zur Basis a .

Hinweise: Eingabe: positive Zahl n und positive Zahl a

Ausgabe: n Pseudoprimzahl zur Basis $a \Rightarrow$ **TRUE**;

n keine Pseudoprimzahl zur Basis $a \Rightarrow$ **FALSE**

im Detail: 1. Ist n gerade, dann ist n keine Pseudoprimzahl. (Nutzen Sie **igcd(?, n)**.)

2. Ist n eine Primzahl, dann ist n keine Pseudoprimzahl.

3. Ist $a^{n-1} \equiv 1 \pmod{n}$, dann ist n eine Pseudoprimzahl zur Basis a .

4. Da $a^{n-1} \not\equiv 1 \pmod{n}$, ist n keine Pseudoprimzahl zur Basis a .

Fragen: 1. Welche der folgenden Zahlen sind Pseudoprimzahlen zur Basis a ? (Angaben: (n, a))
(15, 4), (341, 2), (341, 3), (561, 3), (3608, 4), (5001, 6)

Die Zahlen _____
sind Pseudoprimzahlen zur vorgegebenen Basis a .

3. Pseudoprimzahlen ohne vorgegebene Basis

Erstellen Sie eine Prozedur *isPseudoprime1*, die eine Zahl testet, ob sie eine Pseudoprimzahl ist.

Hinweise: Es reicht, alle Zahlen $a \in \mathbb{N}$ mit $1 < a < n - 1$ zu testen.

Eingabe: positive Zahl n

Ausgabe: n Pseudoprimzahl \Rightarrow **TRUE**, a ; n keine Pseudoprimzahl \Rightarrow **FALSE**

im Detail: Teste alle Zahlen a von 2 bis $n - 2$: Wenn $a^{n-1} \equiv 1 \pmod{n}$, dann ist n eine Pseudoprimzahl.
(Nutzen Sie zur Ausgabe: **return(TRUE, a)**.)

Fragen: 1. Welche der Zahlen sind Pseudoprimzahlen? Geben Sie in Klammern die jeweilige Basis an.
15, 341, 561, 3608, 5001, 7004, 2465, 23001

Die Zahlen _____ sind Pseudoprimzahlen.

2. Welche Basis gibt der Test jeweils aus? _____

Zusatz**1. Liste von Carmichaelzahlen**

Erstellen Sie eine Prozedur *CarmiichaelListe*, die alle Carmichaelzahlen innerhalb eines Intervalls in eine Liste schreibt.

Hinweise: Eingabe: Anfang und Ende des Intervalls
Ausgabe: Liste mit allen Carmichaelzahlen von Anfang bis Ende

im Detail: Nutzen Sie die Prozedur *isCarmichael*

Fragen: 1. Schreiben Sie alle Carmichaelzahlen zwischen 1 und 2000 auf.

-
2. Bei welchen Zahlen zwischen 1 und 1000 versagt der folgende Primzahltest?
Primzahltest: Alle Zahlen kleiner als 2 sind keine Primzahlen.
Gilt für alle $a \in \mathbb{N}$ ($1 < a < n - 1$) mit $\text{ggT}(a, n) = 1$: $a^{n-1} \equiv 1 \pmod{n}$
 $\Rightarrow n$ ist Primzahl
-

2. Liste von Pseudoprimzahlen zu einer vorgegebenen Basis

Erstellen Sie eine Prozedur *PseudoprimeListe*, die alle Pseudoprimzahlen zu einer vorgegebenen Basis innerhalb eines Intervalls in eine Liste schreibt.

Hinweise: Eingabe: Basis a , Anfang und Ende des Intervalls
Ausgabe: Liste mit allen Pseudoprimzahlen zur Basis a von Anfang bis Ende

im Detail: Nutzen Sie die Prozedur *isPseudoprime*

Fragen: 1. Schreiben Sie alle Pseudoprimzahlen zur Basis 6 zwischen 1000 und 2000 auf.

-
2. Welche Zahlen zwischen 1 und 5000 sind Pseudoprimzahlen zu allen Basen 2, 3 und 5?
-

3. Bei welchen Zahlen zwischen 1 und 5000 versagt der folgende Primzahltest?
Primzahltest: Die Zahlen 2, 3 und 5 sind Primzahlen.
Gilt für $a = 2, 3, 5$: $\text{ggT}(a, n) = 1$ und $a^{n-1} \equiv 1 \pmod{n}$
 $\Rightarrow n$ ist Primzahl
-