

# Miller-Rabin-Primzahlentest

Setzen wir

$$B_n = \{a \in \mathbb{Z}_n^* \mid a^{n-1} = 1\}.$$

**Aufgabe 1.** Beweisen Sie folgende Behauptungen.

a)  $B_n$  ist eine Untergruppe der Gruppe  $\mathbb{Z}_n^*$ .

b) Wenn  $n$  eine Primzahl oder Carmichael-Zahl ist, dann gilt  $B_n = \mathbb{Z}_n^*$ .

Wenn  $n$  eine zusammengesetzte und nicht Carmichael-Zahl ist, dann gilt  $|B_n| \leq \frac{1}{2}|\mathbb{Z}_n^*|$ .

c) Sei  $n$  eine ungerade Zahl und  $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ , wobei  $p_1, p_2, \dots, p_r$  verschiedene Primzahlen sind. Dann gilt

$$|B_n| = \prod_{i=1}^r \text{ggT}(n-1, p_i-1).$$

d) Berechnen Sie  $|\mathbb{Z}_n^*|$  und  $|B_n|$  für  $n = 91$  und  $n = 527$ . Finden Sie alle Elemente der Gruppe  $B_n$  für  $n = 91$  und  $n = 527$ .

**Hinweis:** Benutzen Sie den Isomorphismus:

$$\mathbb{Z}_n^* \rightarrow \mathbb{Z}_{p_1^{e_1}}^* \times \dots \times \mathbb{Z}_{p_r^{e_r}}^*.$$

-----

Sei  $n$  eine ungerade Zahl und sei  $n-1 = m2^h$ , wobei  $m$  eine ungerade Zahl ist und  $h \geq 1$  ist. Setzen wir

$$L_n = \{a \in \mathbb{Z}_n^* \mid a^m \equiv 1 \pmod{n} \text{ oder } \exists i, 0 \leq i < h : a^{m2^i} \equiv -1 \pmod{n}\}.$$

Im Allgemeinen ist  $L_n$  keine Untergruppe von  $\mathbb{Z}_n^*$ .

**Aufgabe 2.** Finden Sie eine  $n$ , so daß  $L_n$  keine Untergruppe der Gruppe  $\mathbb{Z}_n^*$  ist.

Nach Monier-Rabin Satz gilt:

- $|L_n| = n-1$ , wenn  $n$  eine Primzahl ist;
- $|L_n| \leq \varphi(n)/4$ , wenn  $n$  eine zusammengesetzte Zahl ist,  $n \neq 9$ .

**Aufgabe 3.**

a) Finden Sie alle Elemente der Menge  $L_n$  für  $n = 91, 527$ .

b) Berechnen Sie  $|L_n|$  für  $n = 561$  (Carmichael-Zahl).

**Aufgabe 4.** a) Mit welcher Wahrscheinlichkeit erhalten wir die Antwort “ $n$  ist eine Primzahl...” im Miller-Rabin-Test für die Zahl  $n = 91$  und den Parameter  $s = 2$ ?

b) Dasselbe Frage für  $n = 561$  und  $s = 1$ .

**Aufgabe 5.** Wiederholen Sie den Miller-Rabin Test 100 Mal (unabhängig) für die Zahl 561 mit dem Parameter  $s = 1$ . Wie viele Male wird der Test die Antwort: “561 ist eine Primzahl ...” zurückgeben?

**Aufgabe 6.** Wenden Sie den Miller-Rabin Test bei folgenden Zahlen an

a) 11111111111111111111,

b)  $\lfloor \pi 10^{37} \rfloor = 31415926535897932384626433832795028841$ .

Welche Antworten erhalten Sie?

**Aufgabe 7.** Prüfen Sie nach, daß folgende Arnault-Zahl eine zusammengesetzte Zahl ist:

A=80383745745363949125707961434194210813883768828755814583748891752229742737653336  
52186502336163960045457915042023603208766569966760987284043965408232928738791850869  
16685732826776177102938969773947016708230428687109997439976544144845341155872450633  
40927902227529622941498423068816854043264575340183297861112989606448452161916528725  
97534901.