3.2 Der strenge Pseudoprimzahltest

Man kann den Pseudoprimzahltest verschärfen, indem man weitere Kennzeichen für Primzahlen auswertet. Sei n zunächst ungerade, zusammengesetzt und keine Primpotenz. Dann gibt es außer ± 1 auch nichttriviale Quadratwurzeln aus 1 in $\mathbb{Z}/n\mathbb{Z}$; findet man eine solche, so hat man nachgewiesen, dass n zusammengesetzt ist. Aber wie soll man nichttriviale Einheitsquadratwurzeln finden, wenn man die Primzerlegung von n nicht kennt? Dazu wird, der Idee aus 2.2 folgend, $n-1$ aufgespalten in $n-1 = 2^s \cdot r$ mit ungeradem r.

Sei $a \in \mathbb{M}_n$. Falls n den Pseudoprimzahltest zur Basis a nicht besteht, ist es als zusammengesetzt erkannt. Andernfalls hat a in der multiplikativen Gruppe $\mathbb{M}_n$ eine Ordnung $\operatorname{Ord}(a) \mid n-1$. In der Folge

$$a^r \bmod n, \quad a^{2r} \bmod n, \quad \ldots, \quad a^{2^s r} \bmod n = 1$$

könnte bereits $a^r \equiv 1 \pmod n$ sein. Dann wird a verworfen, ohne dass eine Entscheidung über n getroffen wird. Andernfalls tritt die 1 erstmals an späterer Stelle auf; das davor stehende Element muß dann Einheitswurzel $\neq 1$ sein. Es kann -1 sein; auch dann wird a ohne Entscheidung verworfen. Andernfalls ist eine nichttriviale Einheitswurzel gefunden und n als zusammengesetzt erkannt. Ist dagegen n prim, so gibt es in dieser Situation stets ein k mit $0 \leq k < s$, so dass

$$a^{2^k r} \equiv -1 \pmod n.$$

Sei nun n eine beliebige positive ganze Zahl, und $n-1$ habe die Zweierordnung s und den ungeraden Teil r. Dann sagt man, n bestehe den **strengen Pseudoprimzahltest zur Basis** a [nach SELFRIDGE ca. 1975], wenn

$$a^r \equiv 1 \pmod n \quad \text{oder} \quad a^{2^k r} \equiv -1 \pmod n \quad \text{für ein } k = 0, \ldots, s-1.$$

Insbesondere gilt dann $a^{n-1} \equiv 1 \pmod n$.

Wir haben also die gleiche Situation wie in Abschnitt 2.3 mit $u = n-1$. Die dortige Menge

$$B_u = \bigcup_{t=0}^{s} \{w \in \mathbb{M}_n \mid w^{r \cdot 2^t} = 1, w^{r \cdot 2^{t-1}} = -1 \text{ (falls } t > 0)\}$$

ist jetzt genau die Menge der Basen, für die n den strengen Pseudoprimzahltest besteht, also die Eigenschaft $(\mathrm{E}_{n,u})$ hat. Diese Basen werden auch **Primzeugen** für n genannt.

Jede Primzahl besteht den strengen Pseudoprimzahltest zu jeder Basis, die kein Vielfaches dieser Primzahl ist. Die CARMICHAEL-Zahl $n = 561$ fällt schon bei $a = 2$ durch: Es ist $n - 1 = 560 = 16 \cdot 35$,

$$2^{35} \equiv 263 \pmod{561}, \qquad 2^{70} \equiv 166 \pmod{561},$$
$$2^{140} \equiv 67 \pmod{561}, \qquad 2^{280} \equiv 1 \pmod{561}.$$

Also ist 561 als zusammengesetzt erkannt. Die kleinste zusammengesetzte Zahl, die den strengen Pseudoprimzahltest für 2, 3 und 5 besteht, ist $25326001 = 2251 \cdot 11251$. Die einzige zusammengesetzte Zahl $< 10^{11}$, die ihn für 2, 3, 5 und 7 besteht, ist 3 215 031 751. Das erweckt die Hoffnung, dass dieser Test zum Erkennen von Primzahlen tatsächlich geeignet ist.

Satz 2 *Sei $n \geq 3$ ungerade. Dann sind äquivalent:*

(i) *n ist prim.*

(ii) *n besteht den strengen Pseudoprimzahltest zu jeder Basis a, die kein Vielfaches von n ist.*

Beweis. „(i) $\Longrightarrow$ (ii)" wurde oben gezeigt.

„(ii) $\Longrightarrow$ (i)": Wegen Satz 1 ist n prim oder eine CARMICHAEL-Zahl, insbesondere $\lambda(n) \mid n - 1 = u$; außerdem ist n quadratfrei, erst recht keine Primpotenz. Also ist der Hilfssatz in 2.3 anwendbar; da nach Voraussetzung $B_u = \mathbb{M}_n$, folgt also, dass n Primpotenz, insgesamt also prim ist. $\diamond$

Korollar 3 *Ist n nicht prim, so gibt es höchstens $\frac{\varphi(n)}{2}$ Basen $< n$, für die n den strengen Pseudoprimzahltest besteht.*

Beweis. Falls n CARMICHAEL-Zahl ist, folgt das aus Satz 1 in 2.3. Andernfalls ist $A_u = \{w \in \mathbb{M}_n \mid w^{n-1} = 1\} < \mathbb{M}_n$ echte Untergruppe, und $B_u \subseteq A_u$. $\diamond$

Bei genauerem Hinsehen kann man sogar die Schranke $\frac{\varphi(n)}{4}$ von RABIN/MONIER herleiten (**Übungsaufgabe**).