§ 15. Spezielle Zahlen

(15.5) Lucas/Lehmer–Test für Mersenne'sche Primzahlen

Die Folge $(u_k)_{k\in\mathbb{N}_0}$ sei rekursiv definiert durch

$$u_0 := 4 \quad , \quad u_{k+1} := u_k^2 - 2 \quad (k \geq 0)\,.$$

Ist dann p eine ungerade Primzahl, so gilt

$$M_p = 2^p - 1 \in \mathbb{P} \quad \Longleftrightarrow \quad u_{p-2} \equiv 0 \pmod{M_p}\,.$$

Dieser Test geht auf Edouard Lucas (1842–1891) zurück und wurde 1930 von Derrick Henry Lehmer (1905–1991) vereinfacht.

C) Pseudoprimzahlen

(15.6) LEMMA: Ist $a \in$ eine beliebige ganze Zahl, so gilt für jede Primzahl $p \in \mathbb{P}$

$$a^p \equiv a \pmod{p}\,.$$

(15.7) BEM: a) Man kann mit (15.6) zeigen, daß eine Zahl nicht prim ist: Gibt es nämlich für $n \in \mathbb{N}$ ein $b \in \mathbb{Z}$ mit $b^n \not\equiv b \bmod n$, so ist n keine Primzahl.

b) Insbesondere gilt $2^n \equiv 2 \pmod{n}$. Zu Zeiten Fermat's glaubte man wohl, daß Zahlen n mit dieser Eigenschaft prim sind. Dies ist nicht verwunderlich, denn

$$\forall\, n \in \mathbb{N} : 2 \leq n \leq 340 \ \wedge \ 2^n \equiv 2 \pmod{n} \quad \Longrightarrow \quad n \in \mathbb{P}\,.$$

Es gilt aber $2^{341} \equiv 2 \pmod{341}$ und $341 = 11 \cdot 31 \notin \mathbb{P}$. (Immerhin hat die Zahl 2^{341} 103 Dezimalstellen!)

(15.8) DEF: Eine zusammengesetzte natürliche Zahl $n \geq 2$ heißt **Pseudoprimzahl**, wenn $2^n \equiv 2 \pmod{n}$ gilt.

(15.9) BEM: a) $n \in \mathbb{N}\,,\, n \geq 2 : \ 2^n \equiv 2 \pmod{n} \ \Longleftrightarrow \ n$ prim pder pseudoprim.

b) 341, 561, 645 sind alle Pseudoprimzahlen ≤ 1000. Diese sind alle ungerade. Pseudoprimzahlen kommen viel seltener vor als Primzahlen:

n	$\pi(n)$	Anz.Pseudopr. $\leq n$	Anz.Carm Z. $\leq n$
10^3	168	3	1
10^6	78 498	247	42

c) $161\,038 = 2 \cdot 73 \cdot 1103$ ist eine gerade Pseudoprimzahl.

d) Frage: Gibt es unendlich viele Pseudoprimzahlen? Antwort: ja (Beweis später).

(15.10) DEF: Sei $b \in \mathbb{Z}$ .Eine zusammengesetzte natürliche Zahl $n \geq 2$ heißt **Pseudoprimzahl zur Basis** b, wenn $b^n \equiv b \pmod{n}$ gilt.

Beispiele: Pseudoprimzahlen zur Basis 2 sind gerade die vorher definierten Pseudoprimzahlen. 341 ist pseudoprim zur Basis 2, nicht aber zur Basis 3 . 91 ist pseudoprim zur Basis 3 , 15 ist pseudoprim zur Basis 4 .

(15.11) LEMMA: Für die Zahl 561 gilt

a) 561 ist nicht prim

b) $b^{561} \equiv b \pmod{561} \;\; \forall\, b \in \mathbb{Z}$.

(15.12) DEF: Eine zusammengesetzte natürliche Zahl $n \geq 2$ heißt **Carmichael–Zahl** , wenn

$$b^n \equiv b \pmod{n}$$

für alle $b \in \mathbb{Z}$ gilt.

Robert Daniel Carmichael (1879–1967), US–amerikanischer Mathematiker

(15.13) BEM: a) Beispiele für Carmichael–Zahlen: $561 = 3 \cdot 11 \cdot 17$, $172\,081 = 7 \cdot 13 \cdot 31 \cdot 61$.

b) $3^{341} \not\equiv 3 \bmod 341$, $3^{645} \not\equiv 3 \bmod 645$. 341 und 645 sind also keine Carmichael Zahlen .

c) $n \geq 2$ zusammengesetzt: n Carmichael–Zahl $\iff$ $b^n \equiv b \pmod{n} \;\; \forall\, b \in \{2, 3, \ldots, n-1\}$

d) Carmichael–Zahlen kommen viel seltener als Pseudoprimzahlen vor (s. Tabelle).

e) Es gibt unendlich viele Carmichael Zahlen (Pommerance/Alford/Granville, 1994) .

(15.14) Pseudoprimzahltest

Seien $n \geq 3$ eine ungerade natürliche Zahl und $T = \{2, 3, \ldots, n-1\}$. Gibt es ein $b \in T$ mit $b^n \not\equiv b \bmod n$, so ist n nicht prim. Gilt dagegen $b^n \equiv b \pmod{n}$ für r zufällig aus T ausgewählte Zahlen, so ist n mit einer gewissen Wahrscheinlichkeit prim. Allerdings versagt das Verfahren, wenn n eine Carmichael Zahl ist.

(15.15) LEMMA: Für $n \in \mathbb{N}$ gilt: $2^n \equiv 2 \pmod{n} \quad \Longrightarrow \quad 2^{M_n} \equiv 2 \pmod{M_n}$.

(15.16) KOROLLAR: a) $n \in \mathbb{N}$ pseudoprim $\quad \Longrightarrow \quad M_n = 2^n - 1$ pseudoprim.

b) Es gibt unendlich viele Pseudoprimzahlen .

c) $p \in \mathbb{P} \quad \Longrightarrow \quad M_p$ ist entweder prim oder pseudoprim.

(15.17) BEM: Die n–te Fermat'sche Zahl $F_n = 2^{2^n} + 1$ $(n \in \mathbb{N}_0)$ ist entweder prim oder pseudoprim.