9. Mersennesche Primzahlen

9.1. Mersenne'sche Primzahlen

Für eine ganze Zahl $n \geqslant 2$ ist $2^n - 1$ höchstens dann eine Primzahl, wenn n prim ist, denn $2^{k\ell} - 1$ ist durch $2^k - 1$ teilbar. Dies folgt aus der Gleichung

$$2^{k\ell} - 1 = (2^k - 1)(2^{k(\ell-1)} + 2^{k(\ell-2)} + \ldots + 1).$$

Nicht alle Zahlen der Form $M_p = 2^p - 1$, p prim, sind Primzahlen. Das erste Gegenbeispiel ist $M_{11} = 2047 = 23 \cdot 89$. Ist jedoch M_p prim, so nennt man es eine *Mersenne'sche Primzahl*.

9.2. Satz (Lucas). *Sei $p \geqslant 3$ prim. Genau dann ist $M_p = 2^p - 1$ eine Primzahl, wenn für die wie folgt rekursiv definierte Folge (v_k) ganzer Zahlen*

$$\begin{aligned} v_0 &:= 4, \\ v_k &:= v_{k-1}^2 - 2, \quad (k \geqslant 1), \end{aligned}$$

gilt: $v_{p-2} \equiv 0 \bmod M_p$.

Vorbemerkung. Die Zahlenfolge $(v_k)_{k\geqslant 0}$ lässt sich im Ring $\mathbb{Z}[\sqrt{3}]$ folgendermaßen ausdrücken:
Sei $\omega := 2 + \sqrt{3}$ und $\overline{\omega} = 2 - \sqrt{3}$. Es ist $\omega + \overline{\omega} = 4$ und $\omega\overline{\omega} = 1$. Damit gilt:

$$v_k = \omega^{2^k} + \overline{\omega}^{2^k}.$$

Beweis durch Induktion nach k.

i) Der *Induktions-Anfang* $k = 0$ ist trivial.

ii) *Induktions-Schritt* $k \to k+1$. Nach Definition ist

$$\begin{aligned} v_{k+1} &= v_k^2 - 2 = \left(\omega^{2^k} + \overline{\omega}^{2^k}\right)^2 - 2 \\ &= \left((\omega^{2^k})^2 + 2 \cdot \omega^{2^k}\overline{\omega}^{2^k} + (\overline{\omega}^{2^k})^2\right) - 2 \\ &= \omega^{2^{k+1}} + 2 + \overline{\omega}^{2^{k+1}} - 2 \;=\; \omega^{2^{k+1}} + \overline{\omega}^{2^{k+1}}, \quad \text{q.e.d.} \end{aligned}$$

Beweis von Satz 9.2.
Wir zeigen hier nur, dass die Bedingung hinreichend ist, d.h.

$$v_{p-2} \equiv 0 \bmod M_p \quad \Longrightarrow \quad M_p \text{ prim.}$$

Angenommen, dies sei nicht der Fall. Dann gibt es eine Primzahl q mit $3 \leqslant q \leqslant \sqrt{M_p}$ und $q \mid M_p$. Es folgt dann

$$v_{p-2} = \omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} \equiv 0 \bmod q.$$

Wir multiplizieren diese Kongruenz mit $\overline{\omega}^{2^{p-2}}$. Wegen $\omega\overline{\omega} = 1$ folgt daraus

$$\omega^{2^{p-1}} \equiv -1 \bmod q.$$

Diese Kongruenz ist als Gleichung im Restklassenring $R := \mathbb{Z}[\sqrt{3}]/q\mathbb{Z}[\sqrt{3}]$ zu verstehen.
Aus dem nachfolgenden Hilfssatz folgt nun, dass ω in der multiplikativen Gruppe $R^\times$ die Ordnung 2^p hat. Da $R = \mathbb{Z}[\sqrt{3}]/q\mathbb{Z}[\sqrt{3}]$ genau q^2 Elemente besitzt, hat $R^\times$ höchstens $q^2 - 1$ Elemente. Da aber

$$2^p = M_p + 1 > q^2,$$

kann es in $R^\times$ kein Element der Ordnung 2^p geben, Widerspruch! Also ist die Annahme falsch, d.h. M_p muss doch eine Primzahl sein.

9.3. Hilfssatz. *Sei G eine multiplikativ geschriebene Gruppe mit Einselement e und $g \in G$ ein Element mit*

$$g^{2^k} = e \quad \textit{und} \quad g^{2^{k-1}} \neq e.$$

Dann hat g die Ordnung 2^k.
Beweis. Aus der Bedingung $g^{2^k} = e$ folgt, dass die Ordnung r von g ein Teiler von 2^k ist, also $r = 2^\ell$ mit $\ell \leqslant k$. Wäre $\ell < k$, würde folgen $g^{2^{k-1}} = e$, im Widerspruch zur Voraussetzung. Also ist $r = 2^k$, q.e.d.