(16.4) SATZ: (Rabin , 1980)

Sei $n > 1$ eine ungerade natürliche Zahl, und es gelte

$$n - 1 \;=\; 2^e \cdot u \;\; (e \geq 1 \;,\; \mathrm{ggT}(u, 2) = 1) \,.$$

Dann sind folgende Aussagen äquivalent:

a) n ist eine Primzahl

b) Für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$ und $a^u \not\equiv 1 \,(\mathrm{mod}\, n)$ gibt es ein $k \in \{0, 1, 2, \ldots, e-1\}$ mit

$$a^{2^k u} \equiv -1 \;(\mathrm{mod}\; n) \,.$$

Für den Beweis von (16.4) (Beweisrichtung "b) $\Longrightarrow$ a)") benötigen wir den folgenden Hilfssatz.

Für $m \in \mathbb{N}$ sei $\quad \nu_2(m) := \;\; \max\{\, k \,|\, k \in \mathbb{N}_0 \,,\, 2^k \,|\, m \,\} \,.$

(16.5) HILFSSATZ: Sei $n > 1$ eine ungerade natürliche Zahl mit der Primfaktorzerlegung $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$ wobei $p_1, p_2, \ldots, p_r$ paarweise verschiedene Primzahlen sind. Ferner sei

$$n - 1 \;=\; 2^e \cdot u \;\; (e \geq 1 \;,\; \mathrm{ggT}(u, 2) = 1) \,.$$

Dann gilt für

$$\nu := \;\; \min\{\, \nu_2(p_i - 1) \,|\, i = 1, 2, \ldots, r \}$$

a) $\nu \leq e$

b) Genau dann ist $\nu = e$, wenn die Zahl

$$|\, \{\, i \,|\, 1 \leq i \leq r \,,\, k_i \text{ ungerade} \,,\, \nu_2(p_i - 1) = \nu \,\} \,|$$

ungerade ist.