7. Übung Elementare Algorithmen in der Algebra

Priv. Doz. Dr. G. Nebe **(SS 00)**

Aufgabe 24. Zeigen Sie, dass $2^x + 1$ zusammengesetzt ist, falls x keine 2-Potenz ist.
Zeigen Sie, dass für $a \geq 2$ die Zahl $a^n - 1$ zusammengesetzt ist, falls entweder $a \neq 2$ oder n keine Primzahl ist.

Aufgabe 25. Zeigen Sie, dass für zusammengesetztes ungerades N die Anzahl der $a \in (\mathbb{Z}/N\mathbb{Z})^*$, für die N eine Pseudoprimzahl zur Basis a ist, $\leq \frac{1}{2}\varphi(N)$ ist.

Aufgabe 26. Zeigen Sie, dass endliche Untergruppen der multiplikativen Gruppe eines Körpers zyklisch sind. Insbesondere sind die Einheitengruppen endlicher Körper zyklisch.

Aufgabe 27. Beweisen Sie Satz (6.26):
Sei N ungerade, $N+1 = \prod_{j=1}^{n} q_j^{\beta_j} \cdot R$ mit paarweise verschiedenen Primzahlen q_j und $q_j \not| R$ $(j = 1, \ldots, n)$ $R < \sqrt{N}$. Gibt es $D \in \mathbb{N}$ mit $ggT(D, N) = 1$ und für alle $j = 1, \ldots, n$ Zahlen $\alpha_j \in \mathbb{Z}/N\mathbb{Z}[\sqrt{D}]^*$ so dass für die Lucas Folge $U^{(j)}$ zu α_j gilt:

$$ggT(U^{(j)}_{(N+1)/q_j}, N) = 1, \quad U^{(j)}_{N+1} \equiv 0 \pmod{N}$$

so ist N eine Primzahl.

Aufgabe 28. Berechnen Sie die folgenden Legendre Symbole:

$$\left(\frac{246}{257}\right), \quad \left(\frac{240}{499}\right), \quad \left(\frac{1234}{257}\right).$$

Abgabe: Donnerstag, den 8.6.00, in der Übung 12:30 Uhr im kl. physik. Hörsaal