5. Übung Elementare Algorithmen in der Algebra

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

Aufgabe 18. Formulieren Sie den Berlekamp Algorithmus zum Faktorisieren quadratfreier Polynome f über $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
Zeigen Sie, dass man mit dem Algorithmus immer eine vollständige Faktorisierung von f in irreduzible Polynome erhält.

Aufgabe 19. Faktorisieren Sie $f(X) = X^8 - 1$ modulo 3^{10}.

Aufgabe 20. Zeigen Sie, dass für $\alpha \geq 2$ die multiplikative Gruppe

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^* = \langle -1 + (2^\alpha\mathbb{Z})\rangle \times \langle 1 + 4 + (2^\alpha\mathbb{Z})\rangle \cong C_2 \times C_{2^{\alpha-2}}.$$

Vorlesung und Übung von Donnerstag, 18.5.00, werden auf Dienstag verschoben,
die Vorlesung von Dienstag findet am Montag, 15.5.00, 13:15-14:45 statt.

Abgabe: Dienstag, den 16.5.00, in der Übung, 14:15 im kl. phys. Hörsaal