

**14.** Sei  $f \in \mathbb{Z}[X]$ ,  $p$  eine Primzahl,  $n \geq 2$ . Zeigen Sie:  $f$  ist genau dann ein Permutationspolynom modulo  $p^n$ , wenn  $f$  ein Permutationspolynom modulo  $p$  ist und  $f'$  keine Nullstellen modulo  $p$  hat.


**15.** Sei  $f \in \mathbb{Z}[X] \setminus \{0\}$  und  $a \in \mathbb{Z}$  mit  $f(a) = f'(a) = 0$ . Sei  $b \in \mathbb{Z}$ , mit  $b \equiv a \pmod{p}$ . Wegen  $f'(a) \equiv 0 \pmod{p}$  und  $f(a) \equiv 0 \pmod{p^2}$  folgt  $f(b) \equiv 0 \pmod{p^2}$ . Durch Iteration erhält man  $f(b) \equiv 0 \pmod{p^n}$ , für alle  $n \in \mathbb{N}$ , und daher  $f(b) = 0$  in  $\mathbb{Z}$ . Daher hat  $f$  unendlich viele Nullstellen. Wo liegt der Fehler in obigem Argument?

**16.** Zeigen Sie: Das Polynom  $X^n + X^m + 1 \in \mathbb{Z}[X]$  besitzt genau dann einen Faktor  $X^2 + X + 1$ , wenn  $n \equiv 1 \pmod{3}$  und  $m \equiv 2 \pmod{3}$  (oder umgekehrt).

**17.** Sei  $f \in \mathbb{Z}[X]$  ein normiertes quadratfreies Polynom. Schreiben Sie eine Funktion, die

- eine Primzahl  $p$  bestimmt, sodass  $f$  quadratfrei modulo  $p$  ist,
- eine Schranke  $S$  bestimmt, sodass die Koeffizienten jedes Faktors von  $g$  von  $f$  in  $\mathbb{Z}[X]$  mit  $\deg g \leq (\deg f)/2$  betragsmäßig kleiner gleich  $S$  sind, und
- die Faktorisierung von  $f$  modulo  $p^n$  bestimmt, für ein  $n$  mit  $p^n \geq 2S + 1$ .

Eventuell bereits geschriebene oder im verwendeten Programm vorhandene Funktionen zur Faktorisierung von Polynomen über endlichen Körpern und zum Liften von Faktorisierungen dürfen verwendet werden.

**18.**  Implementieren Sie den Berlekamp-Zassenhaus-Algorithmus zur Faktorisierung von Polynomen in  $\mathbb{Z}[X]$ .