

**Aufgabe 1: (Berlekamp-Algorithmus)**

Wenden Sie den Berlekamp-Algorithmus an, um folgende Polynome vollständig in  $\mathbb{Z}_p$  zu faktorisieren:

(a)  $a(x) = x^5 + 3x^3 + 2x + 4$  ( $p = 7, 13, 37, 97$ );

(b)  $b(x) = x^{14} + 5x^{10} + 7x^6 + 6x^2 + 1$  ( $p = 7, 13, 17, 37, 97$ );

(c)  $c(x) = x^{105} - 1$  ( $p = 7, 1009$ );

**(8 Punkte)**

**Aufgabe 2: (Swinnerton-Dyer-Polynome)**

Seien

$$SD_n(x) := \prod \left( x \pm \sqrt{2} \pm \sqrt{3} \pm \sqrt{5} \pm \dots \pm \sqrt{p_n} \right),$$

wobei  $p_n$  die  $n$ -te Primzahl bezeichne und sich das Produkt über alle  $2^n$  möglichen Kombinationen von Plus- und Minuszeichen erstreckt, die so genannten *Swinnerton-Dyer-Polynome*.

Man kann zeigen, dass

(a) der Grad von  $SD_n(x)$  genau  $2^n$  beträgt.

(b)  $SD_n(x)$  in  $\mathbb{Z}[x]$  liegt.

(c)  $SD_n(x)$  irreduzibel über  $\mathbb{Z}$  ist.

(d)  $SD_n(x)$ , aufgefasst als Polynom in  $\mathbb{Z}_p[x]$ , für jedes  $p \in \mathbb{P}$  in mindestens  $2^{n-1}$  Faktoren zerfällt.

Programmieren Sie die Berechnung der Swinnerton-Dyer-Polynome und berechnen Sie  $SD_n(x)$  für  $n = 2, \dots, 4$ . Testen Sie die obigen Aussagen (a)-(d) an den drei Beispielpolynomen.

Die Swinnerton-Dyer-Polynome stellen die „schlimmsten“ Eingabepolynome des Berlekamp-Zassenhaus-Algorithmus zur Faktorisierung über  $\mathbb{Z}$  dar, da sie viele Faktoren über  $\mathbb{Z}_p$  besitzen (siehe (d)), aber über  $\mathbb{Z}$  irreduzibel sind (siehe (c)).

**(8 Punkte)**