Aufgabe 1: (Chinesischer Restsatz über $\mathbb{Z}_p[x]$)
Seien die simultanen Kongruenzen

$$\begin{aligned} f(x) &\equiv a_1(x) \mod p_1(x) \\ f(x) &\equiv a_2(x) \mod p_2(x) \\ &\dots \\ f(x) &\equiv a_n(x) \mod p_n(x) \end{aligned}$$

gegeben.

(a) Programmieren Sie den chinesischen Restsatz über $\mathbb{Z}_p[x]$ für den Fall $n = 2$.[1]

(b) Testen Sie ihre Prozedur in $\mathbb{Z}_{19}$ an den simultanen Kongruenzen

$$f(x) \equiv x + 7 \mod x^2 - 11 \quad \text{und} \quad f(x) \equiv x - 7 \mod x^2 - 3.$$

(c) Programmieren Sie den chinesischen Restsatz über $\mathbb{Z}_p[x]$ für $n > 2$ unter Verwendung der Prozedur aus (a). Übergeben werde nun eine Liste der Paare $a_i(x), p_i(x)$. Überlegen Sie sich (mindestens) ein komplexes Kongruenzensystem zum Testen.

Zurückgegeben werde bei (a) und (c) jeweils die gemeinsame Lösung $f(x)$ niedrigsten Grades oder eine Fehlermeldung, falls die Voraussetzungen des Satzes nicht erfüllt sind.

(8 Punkte)

Aufgabe 2: (Fermattest)
Verwenden Sie den kleinen Satz von Fermat, um eine Prozedur zu schreiben, die eine natürliche Zahl auf Primalität testet.
Wenden Sie ihre Prozedur auf die Zahlen

(a) 224743

(b) 46976653

(c) 4463641

(d) 18985773943919701

an und vergleichen Sie mit `PrimeQ`.

(6 Punkte)

Abgabetermin: bis spätestens Donnerstag, 05.06.2008, 08.15 Uhr an sprenger@mathematik.uni-kassel.de.

[1] Nützlich sind hier `PolynomialExtendedGCD` aus dem Algebrapackage und `PolynomialMod`, um die Koeffizienten zu reduzieren.