Maple-Praktikum für Lehramt 2018 - Blatt 6

Dieses Blatt wird in Kalenderwoche 22 (ab 28. Mai) testiert.

Aufgaben: 4

```
> restart;
```

In diesem Blatt wollen wir uns mit Polynomringen und ihren Faktorringen beschäftigen. Dazu sollten Sie zunächst noch einmal einige grundlegenden Begriffe wiederholen.

ÜBUNG [01]:

Geben Sie folgende Definitionen an.
1.) Teiler
2.) größter gemeinsamer Teiler

Aus dem Mathematischen Propädeutikum kennen Sie bereits den euklidischen Algorithmus für ganze Zahlen. Dieser funktioniert nicht nur für den Ring $\mathbb{Z}$ der ganzen Zahlen, sondern für alle *euklidischen Ringe*. Ebenso lassen sich auch die Definitionen eines Teilers und eines größten gemeinsamen eilers übertragen. Wir führen zunächst einige Begriffe ein:

Definition: Ein Ring R heißt *Integritätsbereich*, wenn er nullteilerfrei ist, das heißt, wenn für $a, b \in R$ aus $a \cdot b = 0$ stets folgt, dass $a = 0$ oder $b = 0$.
Ein Integritätsbereich heißt *euklidischer Ring*, wenn es eine Funktion (die *euklidische Funktion*) $f: R \setminus \{0\} \to \mathbb{N}_0$ gibt, so dass für alle $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ existieren mit $a = qb + r$ und $r = 0$ oder $f(r) < f(b)$.

In euklidischen Ringen können wir also eine Division mit Rest durchführen. Somit können wir den euklidischen Algorithmus in allen euklidischen Ringen anweden, denn dieser ist nichts anderes als eine wiederholte Division mit Rest.

ÜBUNG [02]:

1.) Zeigen Sie, dass $\mathbb{Z}$ und $K[x]$ für einen Körper K euklidische Ringe sind, indem Sie die euklidische Funktionen angeben.
2.) Schreiben Sie Prozeduren `eukAlgInt` und `eukAlgPoly`, die den ggT zweier gegebener Ringelemente mit dem euklidischen Algorithmus berechnen. Dabei soll `eukAlgInt` auf dem Ring $\mathbb{Z}$ der ganzen Zahlen und `eukAlgPoly` auf dem Ring $\mathbb{Q}[x]$ der Polynome über den rationalen Zahlen arbeiten. Sie dürfen dabei die Funktionen irem, rem, `iquo` und quo verwenden, nicht aber die in Maple enthaltenen Funktionen zur Bestimmung des ggT.
3.) Bestimmen Sie den größten gemeinsamen Teiler der ganzen Zahlen 12 und 18.
4.) Bestimmen Sie den größten gemeinsamen Teiler der ganzen Zahlen 3681405 und

190281.
5.) Bestimmen Sie den größten gemeinsamen Teiler der Polynome $-20x^6-18x^5-34x^4-23x^3-6x^2-24x+4$ und $8x^5+12x^4+36x^3+20x^2+28x-5$ im Polynomring $\mathbb{Q}[x]$.

In der linearen Algebra haben Sie schon Restklassenringe, also Faktorringe von $\mathbb{Z}$, kennengelernt. Eine solche Konstruktion ist auch mit Polynomringen möglich:

Definition: Sei K ein Körper und $f \in K[x]$. Dann ist $K[x]/fK[x] := \{p + fK[x] \mid p \in K[x]\}$ der *Faktorring* von $K[x]$ modulo f. Dabei ist $p + fK[x] = \{p + f \cdot q \mid q \in K[x]\}$ die Äquivalenzklassen unter der Äquivalenzrelation $a \sim b \Leftrightarrow f \mid a-b$.

ÜBUNG [03]:

Sei K ein Körper und $f \in K[x]$.
1.) Wie können Sie für ein $p \in K[x]$ entscheiden, ob $p + fK[x] \in K[x]/fK[x]$ eine Einheit ist und mit welchem Algorithmus können Sie gegebenenfalls das Inverse bestimmen?

In den folgenden Aufgabenteilen dürfen Sie nicht ^(-1) benutzen, aber die Funktion in Maple, die den Algorithmus aus 1.) durchführt.
2.) Ist 14348906000 invertierbar in $\mathbb{Z}/(3^{115}-1)\mathbb{Z}$ und wenn ja, was ist das Inverse?
3.) Ist 24650347049580675039961314533739438130747265123976009 69 invertierbar in $\mathbb{Z}/(3^{115}-1)\mathbb{Z}$ und wenn ja, was ist das Inverse?
4.) Sei $f := 8x^5+12x^4+36x^3+20x^2+28x-5 \in \mathbb{Q}[x]$. Ist $1+x+f^{42}+f\mathbb{Q}[x]$ invertierbar in $\mathbb{Q}[x]/f\mathbb{Q}[x]$ und wenn ja, was ist das Inverse?
5.) Unter welcher Bedingung an $n \in \mathbb{N}$ ist in $\mathbb{Z}/n\mathbb{Z}$ jedes Element ungleich 0 invertierbar? Erfüllt $n = 2^{2^7}+1$ diese Bedingung?
6.) Unter welcher Bedingung an $f \in \mathbb{Q}[x]$ ist in $\mathbb{Q}[x]/f\mathbb{Q}[x]$ jedes Element ungleich 0 invertierbar? Erfüllt $f = \frac{x^{37}-1}{x-1}$ (Das ist ein Polynom!) dieses Bedingung?

In der nächsten Übung soll es um den chinesischen Restsatz gehen. Er kann benutzt werden, um Systeme von Kongruenzen zu lösen.

Satz (chinesischer Restsatz): Sei R ein euklidischer Ring und seien $m_1,..., m_n \in R \setminus \{0\}$ paarweise teilerfremd. Für Elemente $c_1,..., c_n \in R$ gibt es ein Element $c \in R$, so dass simultan die Kongruenzen $c \equiv c_i \bmod m_i$ für $i = 1,...n$ gelten.

ÜBUNG [04]:

Verwende die Bezeichnungen aus obigem Satz. Sei weiter $P := \prod_{i=1}^{n} m_i$ sowie $P_i := P / m_i$ und $x_i \in R$ mit $x_i P_i \equiv 1 \bmod m_i$ für $i = 1,..., n$.

1.) Wie können die x_i aus $m_1,..., m_n$ berechnet werden?

2.) Warum erfüllt $c := \sum_{i=1}^{n} c_i x_i P_i$ die gewünschten Kongruenzen?

3.) Warum ist c eindeutig modulo P? *Hinweis: Wenn c' eine weitere Lösung ist, was ist dann mit $c - c'$?*

4.) Schreiben Sie eine Prozedur für den Fall $R = \mathbb{Z}$ in Maple, die zwei Listen $[m_1,..., m_n]$ (paarweise teilerfremd) und $[c_1,..., c_n]$ als Eingabe erhält und eine Lösung $c \in \mathbb{Z}$ der simultanen Kongruenzen $c \equiv c_i \bmod m_i$ für $i = 1,..., n$ zurückgibt. Schreiben Sie Ihre Funktion so, dass die Ausgabe betragsmäßig möglichst klein ist, also zwischen $-\frac{P+1}{2}$ und $\frac{P+1}{2}$ liegt.

5.) Bestimmen Sie ein $c \in \mathbb{Z}$ mit $c \equiv 74540892843699 \bmod 800187484459$, $c \equiv 437395175522 \bmod 22424170465$ und $c \equiv 21501059632462 \bmod 427552056869$.