Division mit Rest - der heimliche Hauptsatz der Algebra

Franz Pauer

Institut für Mathematik, Universität Innsbruck,
Technikerstr. 25, A-6020 Innsbruck, Österreich.
Franz.Pauer@uibk.ac.at

3. Juni 2004

1 Einleitung

Die Themen „Rechnen mit ganzen (und rationalen) Zahlen“ und „Rechnen mit Polynomen“ spielen im Mathematikunterricht an höheren Schulen eine zentrale Rolle. Die Theorie dieser zwei Teilgebiete der Algebra verläuft weitgehend parallel, Aufgaben und Sätze des einen Gebietes haben meistens ein Analogon im anderen. In diesem Beitrag soll diese Parallelität verdeutlicht und der Grund dafür aufgezeigt werden: sowohl für das Rechnen mit ganzen Zahlen als auch für das Rechnen mit Polynomen gibt es *einen* grundlegenden Satz und *einen* grundlegenden Algorithmus, nämlich den *Satz über die Division mit Rest* (für Zahlen und für Polynome) und den *Divisionsalgorithmus*.

Wir betrachten zu Beginn einige einfach formulierbare Aufgaben (in der linken Spalte für Zahlen, in der rechten für Polynome), deren systematische Lösung in den folgenden Abschnitten besprochen wird.

Aufgaben

N sei die Anzahl der Euromünzen in einem Sack. Berechne die Ziffern von N zur Basis 10 und zur Basis 2 !	Berechne Bruchzahlen c_0, c_1, c_2, c_3 so, dass $x^3 + 2x^2 - 3x + 1 =$ $c_3(x-1)^3 + c_2(x-1)^2 + c_1(x-1) + c_0$ ist!
Kürze $\frac{1243168}{1832051}$!	Kürze $\frac{2x^4-3x^3-7x^2-3x-9}{2x^5+x^4-3x^3+4x^2+4x-3}$!
	Berechne die Anzahl der Nullstellen von $x^7+2x^6-2x^3+3x^2-\frac{11}{4}x^5-\frac{3}{2}x+\frac{3}{4}x^4+\frac{1}{4}$!
Berechne ganze Zahlen u und v so, dass $187u + 102v = 34$ ist!	Berechne Polynome f und g so, dass $(x^4 - 2x^2 + x - 5)f + (x^5 + x^3 - 5)g =$ $= x^2 + x - 5$ ist !
Finde eine ganze Zahl z so, dass der Rest von $18z$ nach Division durch 23 gleich 1 ist!	Finde Bruchzahlen s, t, u so, dass $\frac{1}{\sqrt[3]{4}+3\sqrt[3]{2}+2} = s\sqrt[3]{4} + t\sqrt[3]{2} + u$ ist!

2 Division mit Rest von Zahlen

Wie üblich bezeichnen wir mit

$$\mathbb{N} := \{0, 1, 2, \ldots\}$$

und mit

$$\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

die Mengen der natürlichen Zahlen und der ganzen Zahlen. Wir setzen die Addition $+$, Multiplikation $\cdot$, Ordnung $\leq$ und die Rechenregeln dazu (wie zum Beispiel „$(a + b) \cdot c = a \cdot c + b \cdot c$“ oder „aus $a \leq b$ folgt $a + c \leq b + c$“) als bekannt voraus. In der Algebra werden diese Voraussetzungen mit „$(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring“ und „die Rechenoperationen $+$ und $\cdot$ sind mit der Ordnung $\leq$ verträglich“ kurz zusammengefasst.

Jeder, der einmal den Inhalt eines Sackes voller Zuckerln auf b Kinder gerecht verteilt hat, hat schon einmal mit Rest durch b dividiert: Man schaut zuerst nach, ob im Sack mindestens b Zuckerln sind. Wenn nicht, fängt man mit dem Verteilen gar nicht an. Andernfalls gibt man jedem Kind ein Zuckerl, die Anzahl der Zuckerln im Sack ist dadurch um b kleiner geworden. Diesen Vorgang wiederholt man so lange, bis im Sack weniger als b Zuckerln sind. Sobald die Anzahl der Zuckerln im Sack kleiner als b ist, ist diese Anzahl der Rest und die Anzahl der Zuckerln, die jedes Kind bekommen hat, ist der ganzzahlige Quotient.

Formal sieht das so aus:

Satz 1. (Division mit Rest von ganzen Zahlen)
Zu je zwei natürlichen Zahlen a und b mit $b \neq 0$ gibt es eindeutig bestimmte natürliche Zahlen m und r mit den Eigenschaften

$$a = m \cdot b + r \quad \textit{und} \quad 0 \leq r < b\,.$$

Die Zahl m heißt ganzzahliger Quotient *von a und b, die Zahl r* Rest *von a nach Division durch b.*

Divisionsalgorithmus (Berechnung von m und r):

- Setze $m := 0$ und $r := a$.
- Solange $r \geq b$ ist, ersetze r durch $r - b$ und m durch $m + 1$.

Die Bedeutung dieses Satzes liegt darin, dass die drei „Strukturen“ $+, \cdot$ und $\leq$ auf $\mathbb{Z}$ zueinander in Beziehung gesetzt werden.

3 Eine erste Anwendung: Darstellung von Zahlen durch Ziffern

Nehmen wir an, Sie kommen mit einem Sack voller Euromünzen in eine Bank und wollen dieses Geld auf ihr Sparbuch einzahlen. Die Anzahl der Euromünzen im Sack ist eine eindeutig bestimmte natürliche Zahl N. Bevor diese Zahl in Ihr Sparbuch eingetragen werden kann, muss der Bankbeamte ihre *Zifferndarstellung* (zur Basis 10) berechnen. Eine Zahl ist also nicht immer schon in Zifferndarstellung gegeben, sondern diese ist eine „Zusatzinformation“ über die Zahl. Wie wird die Zifferndarstellung zur Basis 10 von N ermittelt? Man bildet aus den Euromünzen solange „Zehnerstapel“, bis nur noch weniger als zehn Münzen übrigbleiben, das heißt: N wird mit Rest durch 10 dividiert. Die Anzahl der übriggebliebenen Euromünzen ist dann die „Einerziffer“ von N. Macht man dasselbe nun mit den Zehnerstapeln statt mit den Münzen, dann erhält man die „Zehnerziffer“ von N, usw.

Satz 2. *Seien a und b positive ganze Zahlen und $b \geq 2$. Dann gibt es eindeutig bestimmte natürliche Zahlen $n, z_0, z_1, \ldots, z_n$ so, dass*

$$z_n \neq 0,\ 0 \leq z_0, z_1, \ldots, z_n < b$$

und

$$a = z_n b^n + z_{n-1} b^{n-1} + \ldots + z_1 b^1 + z_0$$

ist.
Wenn b fest gewählt ist, dann ist a durch die Zahlen $n, z_0, z_1, \ldots, z_n$ eindeutig bestimmt. Man wählt Zeichen für die Zahlen von 0 bis $b - 1$ und schreibt dann

$$z_n z_{n-1} \ldots z_0$$

statt

$$z_n b^n + z_{n-1} b^{n-1} + \ldots + z_1 b^1 + z_0\,.$$

Die Zahlen $z_0, z_1, \ldots, z_n$ heißen Ziffern von a zur Basis b *(für $b = 2$ „Binärziffern“, für $b = 10$ „Dezimalziffern“).*

Algorithmus zur Berechnung der Ziffern Die Ziffern z_i von $a \neq 0$ zur Basis b können mit dem folgenden Verfahren berechnet werden:

- Setze $i := 0$.
- Solange a nicht 0 ist: Die i-te Ziffer z_i ist der Rest von a nach Division durch b. Ersetze a durch den ganzzahligen Quotienten von a und b. Ersetze i durch $i + 1$.

4 Polynomfunktionen und Polynome

Mit $\mathbb{Q}$ bezeichnen wir die Menge

$$\{\frac{a}{b} \mid a, b \in \mathbb{Z},\, b \neq 0\}$$

der *rationalen Zahlen* (oder *Bruchzahlen*). Seien $n \in \mathbb{N}$ und $a_0, a_1, \ldots, a_n \in \mathbb{Q}$. Dann ist die Funktion

$$f : \mathbb{Q} \to \mathbb{Q}\,,$$

$$z \mapsto a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n = \sum_{i=0}^{n} a_i z^i\,,$$

eine *Polynomfunktion* von $\mathbb{Q}$ nach $\mathbb{Q}$. Die Zahlen $a_0, \ldots, a_n$ sind die *Koeffizienten von* f. Die endliche Folge $a := (a_0, \ldots, a_n)$ heißt *Polynom*. Wir schreiben für a im weiteren

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \text{ oder } \sum_{i=0}^{n} a_i x^i$$

und sprechen dann von einem *Polynom in der Variablen x mit Koeffizienten in* $\mathbb{Q}$. Für die Menge dieser Polynome schreiben wir $\mathbb{Q}[x]$.

Wenn $a_n \neq 0$ ist, ist $grad(a) := n$ der *Grad* von f und $lk(a) := a_n$ der *Leitkoeffizient* von a.

Durch das Polynom a ist die Polynomfunktion f eindeutig bestimmt. Weil $\mathbb{Q}$ eine unendliche Menge ist, kann aus Abschnitt 8 leicht abgeleitet werden, dass auch die Koeffizienten $a_0, a_1, \ldots, a_n$ durch die Polynomfunktion f eindeutig bestimmt sind. Wir können im weiteren daher ein Polynom und die entsprechende Polynomfunktionen als gleich auffassen.

Für die Addition

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i := \sum_{i=0}^{n} (a_i + b_i) x^i$$

und die Multiplikation

$$(\sum_{i=0}^{n} a_i x^i) \cdot (\sum_{i=0}^{n} b_i x^i) := \sum_{i=0}^{2n} (\sum_{j=0}^{i} a_j \cdot b_{i-j}) x^i$$

(mit $a_i := 0, b_i := 0$ für $i > n$) gelten die gleichen Rechenregeln wie für die Addition und Multiplikation von ganzen Zahlen, genauer: $(\mathbb{Q}[x], +, \cdot)$ ist ein kommutativer Ring. Die Rolle der Ordnung $\leq$ auf $\mathbb{Z}$ wird (in gewisser Hinsicht) von der durch den Grad bestimmten Teilordnung übernommen.

5 Division mit Rest von Polynomen

(vergleiche Abschnitt 2)

Satz 3. (Division mit Rest von Polynomen)
Zu je zwei Polynomen a und b mit $b \neq 0$ gibt es eindeutig bestimmte Polynome m und r mit den Eigenschaften

$$a = m \cdot b + r \quad \textit{und} \quad [r = 0 \textit{ oder } grad(r) < grad(b)] \,.$$

Das Polynom m heißt polynomialer Quotient *von a und b, das Polynom r* Rest *von a nach Division durch b.*

Divisionsalgorithmus (Berechnung von m und r):

- Setze $m := 0$ und $r := a$.
- Solange $r \neq 0$ und $grad(r) \geq grad(b)$ ist, ersetze r durch $r - h \cdot b$ und m durch $m + h$, wobei

$$h := lk(r) \cdot lk(b)^{-1} \cdot x^{grad(r)-grad(b)} \text{ ist.}$$

Der Grad von $r - h \cdot b$ ist kleiner als der Grad von r, weil (nach Definition von h) die Grade und die Leitkoeffizienten von r und $h \cdot b$ gleich sind. Würde man (wie bei Zahlen) r nur durch die Differenz $r - b$ ersetzen, wäre das nicht der Fall und der Algorithmus würde nicht nach endlich vielen Schritten enden.

Der Zifferndarstellung bei Zahlen entspricht der folgende Satz:

Satz 4. *Seien a und b Polynome $\neq 0$ und $grad(b) \geq 1$. Dann gibt es eine eindeutig bestimmte natürliche Zahl n und Polynome $z_0, z_1, \ldots, z_n$ so, dass*

$$(z_0 = 0 \textit{ oder } grad(z_0) < grad(b)), \ldots, (z_{n-1} = 0 \textit{ oder } grad(z_{n-1}) < grad(b)),$$

$$z_n \neq 0 \textit{ und } grad(z_n) < grad(b)$$

und

$$a = z_n b^n + z_{n-1} b^{n-1} + \ldots + z_1 b^1 + z_0$$

ist.

Algorithmus zur Berechnung der Polynome $z_0, \ldots, z_n$

- Setze $i := 0$.
- Solange a nicht 0 ist: Das Polynom z_i ist der Rest von a nach Division durch b. Ersetze a durch den polynomialen Quotienten von a und b. Ersetze i durch $i + 1$.

Beispiel 5. Sei $a := x^3 + 2x^2 - 3x + 1$ und $b := x - 1$. Wir berechnen die Polynome $z_0, \ldots, z_3$ mit dem Computeralgebrasystem Maple 9. Mit rem(a,b,x) wird der Rest von a nach Division durch b berechnet, mit quo(a,b,x) der polynomiale Quotient von a und b.

```
> a:=x^3+2*x^2-3*x+1;
```

$$a := x^3 + 2\,x^2 - 3\,x + 1$$

```
> b:=x-1;
```

$$b := x - 1$$

```
> z_0:=rem(a,b,x);
```

$$z\_0 := 1$$

```
> a1:=quo(a,b,x);
```

$$a1 := x^2 + 3\,x$$

```
> z_1:=rem(a1,b,x);
```

$$z\_1 := 4$$

```
> a2:=quo(a1,b,x);
```

$$a2 := x + 4$$

```
> z_2:=rem(a2,b,x);
```

$$z\_2 := 5$$

```
> a3:=quo(a2,b,x);
```

$$a3 := 1$$

```
> z_3:=rem(a3,b,x);
```

$$z\_3 := 1$$

Also: $x^3 + 2x^2 - 3x + 1 = (x-1)^3 + 5(x-1)x^2 + 4(x-1) + 1$.

6 Der größte gemeinsame Teiler von zwei Zahlen

Seien a, b, c ganze Zahlen, alle $\neq 0$. Dann ist

$$\frac{a}{b} = \frac{a \cdot c}{b \cdot c} \in \mathbb{Q}\,.$$

Der Übergang von

$$\frac{a \cdot c}{b \cdot c} \text{ nach } \frac{a}{b}$$

heißt *durch c kürzen*.
Kürze „bestmöglich“!

Der *größte gemeinsame Teiler* von zwei von Null verschiedenen ganzen Zahlen ist die größte ganze Zahl, die beide teilt.

Es sei $a \neq c \cdot b$. Dann ist

$$ggT(a, b) = ggT(a - c \cdot b, b)\,,$$

insbesondere (falls $a \neq b$ ist)

$$ggT(a, b) = ggT(a - b, b)\,.$$

Satz 6. (Euklidischer Algorithmus für ganze Zahlen) *Mit dem folgenden Verfahren kann der größte gemeinsame Teiler von positiven ganzen Zahlen a und b berechnet werden:*

- *Solange die zwei Zahlen verschieden sind, ersetze die größere durch die Differenz der größeren und der kleineren.*
- *Wenn die zwei Zahlen gleich sind, dann ist diese Zahl der $ggT(a, b)$.*

Ersetzt man mehrfaches Abziehen derselben Zahl durch eine Division mit Rest, dann hat dieses Verfahren die folgende Form:

- Solange keine der zwei Zahlen ein Teiler der anderen ist, ersetze die größere der zwei Zahlen durch ihren Rest nach Division durch die kleinere.
- Wenn eine der zwei Zahlen ein Teiler der anderen ist, dann ist sie der $ggT(a, b)$.

In Maple wird mit igcd(a,b) der größte gemeinsame Teiler der ganzen Zahlen a und b berechnet, mit iquo(a,b) der ganzzahlige Quotient von a und b.

Beispiel 7.

```
> igcd(1243168,1832051);
```

$$53$$

```
> iquo(1243168,53);
```

$$23456$$

```
> iquo(1832051,53);
```

$$34567$$

Die Bruchzahl $\frac{1243168}{1832051}$ kann also einfacher durch $\frac{23456}{34567}$ dargestellt werden.

7 Der größte gemeinsame Teiler von zwei Polynomen

Die Überlegungen des letzten Abschnittes für ganze Zahlen können direkt auf Polynome übertragen werden:

Seien a, b, c Polynome, alle $\neq 0$. Dann ist

$$\frac{a}{b} = \frac{a \cdot c}{b \cdot c} \, .$$

Der Übergang von

$$\frac{a \cdot c}{b \cdot c} \text{ nach } \frac{a}{b}$$

heißt *durch c kürzen*.
Kürze „bestmöglich“!

Der *größte gemeinsame Teiler* von zwei von Null verschiedenen Polynomen ist das Polynom größten Grades, das beide teilt und dessen Leitkoeffizient 1 ist.

Es sei $a \neq c \cdot b$. Dann ist

$$ggT(a, b) = ggT(a - c \cdot b, b) \, .$$

Satz 8. (Euklidischer Algorithmus für Polynome) *Mit dem folgenden Verfahren kann der größte gemeinsame Teiler von a und b berechnet werden:*

- *Solange keines der zwei Polynome ein Teiler des anderen ist, ersetze das Polynom größeren (oder gleichen) Grades durch seinen Rest nach Division durch das andere.*
- *Wenn eines der zwei Polynome ein Teiler der anderen ist, dann ist es (nach Division durch den Leitkoeffizienten) der $ggT(a, b)$.*

In Maple wird mit gcd(a,b) der größte gemeinsame Teiler der Polynome a und b berechnet, mit quo(a,b,x) der polynomiale Quotient von a und b.

Beispiel 9.

```
> gcd(2*x^4-3*x^3-7*x^2-3*x-9,2*x^5+x^4+4*x^2+4*x-3*x^3-3);
```

$$2\,x+3$$

```
> quo(2*x^4-3*x^3-7*x^2-3*x-9,2*x+3,x);
```

$$x^3-3\,x^2+x-3$$

```
> quo(2*x^5+x^4+4*x^2+4*x-3*x^3-3,2*x+3,x);
```

$$x^4-x^3+2\,x-1$$

Die rationale Funktion $\frac{2x^4-3x^3-7x^2-3x-9}{2x^5+x^4-3x^3+4x^2+4x-3}$ kann also einfacher durch $\frac{x^3-3x^2+x-3}{x^4-x^3+2x-1}$ dargestellt werden.

8 Die Anzahl der Nullstellen eines Polynoms

Sei $a := \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$. Dann ist

$$Da := \sum_{i=1}^{n} i a_i x^{i-1}$$

die *Ableitung* von f.

Im allgemeinen ist es nicht möglich, die komplexen Nullstellen eines Polynoms (exakt) zu berechnen. Aber: die Anzahl seiner Nullstellen (ohne Vielfachheiten) kann leicht berechnet werden. Auch der Beweis des folgenden Satzes ist nicht schwierig.

Satz 10. *Die Anzahl der Nullstellen von a in $\mathbb{C}$ ist*

$$grad(a) - grad(ggT(a, Da)) \; .$$

In Maple wird mit diff(a,x) die Ableitung des Polynoms a berechnet und mit degree(a,x) der Grad von a.

Beispiel 11.

```
> a:=x^7+2*x^6-2*x^3+3*x^2-11/4*x^5-3/2*x+3/4*x^4+1/4;
```

$$a := x^7+2\,x^6-2\,x^3+3\,x^2-\frac{11}{4}\,x^5-\frac{3}{2}\,x+\frac{3}{4}\,x^4+\frac{1}{4}$$

```
> diff(a,x);
```

$$7\,x^6+12\,x^5-6\,x^2+6\,x-\frac{55}{4}\,x^4-\frac{3}{2}+3\,x^3$$

```
> gcd(a,diff(a,x));
```

$$-\frac{1}{2}+x$$

```
> degree(a,x);
```

$$7$$

```
> degree(a,x)-degree(gcd(a,diff(a,x)),x);
```

$$6$$

Das Polynom a hat also genau 6 Nullstellen in $\mathbb{C}$.

9 Ganzzahlige lineare Gleichungen

Satz 12. *Es seien a und b positive ganze Zahlen. Es gibt ganze Zahlen u, v so, dass*

$$u \cdot a + v \cdot b = ggT(a, b)$$

ist. Diese können mit dem folgenden Verfahren (Erweiterter Euklidischer Algorithmus) berechnet werden:

- *Setze $A := (A_1, A_2, A_3) := (a, 1, 0)$ und $B := (B_1, B_2, B_3) := (b, 0, 1)$.*
- *Solange B_1 die Zahl A_1 nicht teilt, berechne den ganzzahligen Quotienten m von A_1 und B_1 und setze $C := B$, $B := A - m \cdot C :=$ $= (A_1 - m \cdot C_1, A_2 - m \cdot C_2, A_3 - m \cdot C_3)$ und $A := C$.*
- *Wenn B_1 die Zahl A_1 teilt, dann ist $u := B_2$ und $v := B_3$.*

Satz 13. *Seien a, b, c ganze Zahlen, alle $\neq 0$.*
Es gibt genau dann ganze Zahlen u, v mit $a \cdot u + b \cdot v = c$, wenn $ggT(a, b)$ ein Teiler von c ist.

In Maple werden mit igcdex(a,b,u,v) der größte gemeinsame Teiler $ggT(a, b)$ der Zahlen a und b berechnet und darüberhinaus Zahlen u und v mit $ggT(a, b) = a \cdot u + b \cdot v$.

Beispiel 14. Berechne ganze Zahlen u und v so, dass $187u + 102v = 34$ ist!

```
> igcdex(187,102,u1,v1);
```
$$17$$
```
> u1;
```
$$-1$$
```
> v1;
```
$$2$$
```
> irem(34,17);
```
$$0$$
```
> iquo(34,17);
```
$$2$$
```
> u:=2*u1;
```
$$u := -2$$
```
> v:=2*v1;
```
$$v := 4$$
```
> -2*187+4*102;
```
$$34$$

Daher ist $187 \cdot (-2) + 102 \cdot 4 = 34$.

10 Polynomiale lineare Gleichungen

Satz 15. *Es seien a, b Polynome, beide $\neq 0$. Es gibt Polynome u, v so, dass*

$$u \cdot a + v \cdot b = ggT(a, b)$$

ist. Diese können mit dem folgenden Verfahren (Erweiterter Euklidischer Algorithmus) berechnet werden:

- *Setze $A := (A_1, A_2, A_3) := (a, 1, 0)$ und*
  $B := (B_1, B_2, B_3) := (b, 0, 1)$.
- *Solange B_1 das Polynom A_1 nicht teilt, berechne den polynomialen Quotienten m von A_1 und B_1 und setze $C := B$, $B := A - m \cdot C :=$*
  $= (A_1 - m \cdot C_1, A_2 - m \cdot C_2, A_3 - m \cdot C_3)$ *und $A := C$.*
- *Wenn B_1 das Polynom A_1 teilt, dann ist*
  $u := lk(B_1)^{-1} \cdot B_2$ *und* $v := lk(B_1)^{-1} \cdot B_3$.

Satz 16. *Seien a, b, c Polynome, alle $\neq 0$.*
Es gibt genau dann Polynome u, v mit $a \cdot u + b \cdot v = c$, wenn $ggT(a, b)$ ein Teiler von c ist.

In Maple werden mit gcdex(a,b,u,v) der größte gemeinsame Teiler $ggT(a, b)$ der Polynome a und b berechnet und darüberhinaus Polynome u und v mit $ggT(a, b) = a \cdot u + b \cdot v$.

Beispiel 17. Berechne Polynome f und g so, dass
$(x^4 - 2x^2 + x - 5)f + (x^5 + x^3 - 5)g = x^2 + x - 5$ ist !

```
> gcdex(x^4-2*x^2+x-5,x^5+x^3-5,x,f1,g1);
```

$$1$$

```
> f1;
```

$$-\frac{31}{539} - \frac{71}{2695}\,x^2 + \frac{3}{539}\,x - \frac{39}{2695}\,x^4 - \frac{136}{2695}\,x^3$$

```
> g1;
```

$$-\frac{384}{2695} - \frac{46}{2695}\,x + \frac{136}{2695}\,x^2 + \frac{39}{2695}\,x^3$$

```
> f2:=(x^2+x-5)*f1;
```

$$f2 := (x^2 + x - 5)\,(-\frac{31}{539} - \frac{71}{2695}\,x^2 + \frac{3}{539}\,x - \frac{39}{2695}\,x^4 - \frac{136}{2695}\,x^3)$$

```
> g2:=(x^2+x-5)*g1;
```

$$g2 := (x^2 + x - 5)\,(-\frac{384}{2695} - \frac{46}{2695}\,x + \frac{136}{2695}\,x^2 + \frac{39}{2695}\,x^3)$$

11 Restklassenringe

Sei n eine ganze Zahl ≥ 2.
Die Menge $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$ mit der Addition

$$a +_n b := \text{ Rest von } a + b \text{ nach Division durch } n$$

und der Multiplikation

$$a \cdot_n b := \text{ Rest von } a \cdot b \text{ nach Division durch } n$$

heißt „Restklassenring $\mathbb{Z}$ modulo n“. Diese Restklassenringe finden zum Beispiel in der Kodierungstheorie oder bei Verfahren zum „schnellen Rechnen“ Anwendung.

Kann in $\mathbb{Z}_n$ dividiert werden? Das heißt: Gibt es zu $a \in \mathbb{Z}_n$ eine Zahl $b \in \mathbb{Z}_n$ mit $a \cdot_n b = 1$?

Das ist genau dann der Fall, wenn $ggT(a, n) = 1$ ist: Dann gibt es nämlich Zahlen u und v so, dass $u \cdot a + v \cdot n = 1$ ist (siehe Abschnitt 9). Division mit Rest von u durch n ergibt $u = m \cdot n + r$ mit $0 \leq r < n$.
Daraus erhält man $r \cdot a + (v + m \cdot a) \cdot n = 1$, also $r \cdot_n a = 1$.

Falls n eine Primzahl ist, ist $ggT(a, n) = 1$ für alle $0 < a < n$, also ist dann $\mathbb{Z}_n$ ein Körper.

Beispiel 18. Finde eine ganze Zahl z so, dass der Rest von $18z$ nach Division durch 23 gleich 1 ist!

```
> igcdex(18,23,u,v);
                                1
> u;
                                9
> irem(18*9,23);
                                1
```

12 Algebraische Zahlen

Sei h ein Polynom in $\mathbb{Q}[x]$ mit $grad(h) \geq 1$.
Die Menge $\mathbb{Q}[x]/h := \{$ Polynome vom Grad $< grad(h)\} \cup \{0\}$ mit der Addition

$$a +_h b := \text{ Rest von } a + b \text{ nach Division durch } h$$

und der Multiplikation

$$a \cdot_h b := \text{ Rest von } a \cdot b \text{ nach Division durch } h$$

heißt „Restklassenring $\mathbb{Q}[x]$ modulo h “. Diese Restklassenringe finden zum Beispiel zur Konstruktion von Körpererweiterungen von $\mathbb{Q}$, in denen irreduzible Polynome in $\mathbb{Q}[x]$ Nullstellen haben, Anwendung.

Kann in $\mathbb{Q}[x]/h$ dividiert werden? Das heißt: Gibt es zu $a \in \mathbb{Q}[x]/h$ ein Polynom $b \in \mathbb{Q}[x]/h$ mit $a \cdot_h b = 1$?

Das ist genau dann der Fall, wenn $ggT(a, h) = 1$ ist: Dann gibt es nämlich Polynome u und v so, dass $u \cdot a + v \cdot h = 1$ ist (siehe Abschnitt 10). Division mit Rest von u durch h ergibt $u = m \cdot h + r$, $r = 0$ oder $grad(r) < grad(h)$.
Daraus erhält man $r \cdot a + (v + m \cdot a) \cdot h = 1$, also $r \cdot_h a = 1$.

Falls h ein irreduzibles Polynom ist, ist $ggT(f, h) = 1$ für alle $f \neq 0$ mit $grad(f) < grad(h)$, also ist dann $\mathbb{Q}[x]/h$ ein Körper.

Das Polynom h hat in diesem Körper eine Nullstelle, und zwar x.

Beispiel 19. Finde Bruchzahlen s, t, u so, dass

$$\frac{1}{\sqrt[3]{4}+3\sqrt[3]{2}+2} = s\sqrt[3]{4}+t\sqrt[3]{2}+u$$

ist!
Sei $h := x^3-2$ und $a := x^2+x+2$. Wir schreiben $\sqrt[3]{2}$ für die Nullstelle x von h in $\mathbb{Q}[x]/h$.

```
> h:=x^3-2;
```

$$h := x^3-2$$

```
> f:=x^2+3*x+2;
```

$$a := x^2+3\,x+2$$

```
> gcdex(a,h,x,u,v);
```

$$1$$

```
> u;
```

$$-\frac{1}{15}-\frac{2}{15}\,x+\frac{7}{30}\,x^2$$

```
> rem(u*f,h,x);
```

$$1$$

Also ist

$$f\cdot_h(\frac{7}{30}x^2-\frac{2}{15}x-\frac{1}{15})=1$$

in $\mathbb{Q}[x]/h$, somit

$$\frac{1}{\sqrt[3]{4}+\sqrt[3]{2}+2} = \frac{7}{30}\sqrt[3]{4}-\frac{2}{15}\sqrt[3]{2}-\frac{1}{15}\,.$$