# Division mit Rest -
# der heimliche Hauptsatz der Algebra

Franz Pauer
Institut für Mathematik, Universität Innsbruck,
Technikerstr. 13, A-6020 Innsbruck, Österreich.
Franz.Pauer@uibk.ac.at

Lehrer/innen/fortbildungstag „West“
der Österreichischen Mathematischen Gesellschaft
2009

Salzburg, 2. April 2009

Rechnen mit **ganzen** (u. rationalen) **Zahlen**

Satz $(+, \cdot, \leq)$

Rechnen mit **Polynomen** (u. rationalen Funktionen)

Satz $(+, \cdot, grad)$

**Division mit Rest**

Zu zwei ganzen Zahlen bzw. Polynomen
$a, b$ mit $b \neq 0$
gibt es eindeutig bestimmte
ganze Zahlen bzw. Polynome $m$ und $r$ mit
$a = m \cdot b + r$ und
$0 \leq r < |b|$ bzw. ($r = 0$ oder $grad(r) < grad(b)$).

$m$ heißt *ganzzahliger bzw. polynomialer Quotient*
von $a$ und $b$,
$r$ heißt *Rest* von $a$ nach Division durch $b$.

## Aufgaben

- $N$ sei die Anzahl der Euromünzen in einem Sack. Berechne die Ziffern von $N$ zur Basis 10 und zur Basis 2 !

  Sei $f = \sum_{i=0}^{n} c_i x^i$ ein Polynom.
  Berechne Polynome $a_i x + b_i$, $0 \leq i \leq m$, so, dass

  $$f = \sum_{i=0}^{m} (a_i x + b_i)(x^2 + 1)^i$$

  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 in $\mathbb{C}$ 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 $u$ und $v$ so, dass

$$(x^4-2x^2+x-5)u+(x^5+x^3-5)v = x^2+x-5$$

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 !

## Division mit Rest von ganzen Zahlen

**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*

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

$m$ *. . . ganzzahliger Quotient von* $a$ *und* $b$
$r$ *. . . 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* $m + 1$*.*

## Darstellung von Zahlen durch Ziffern

**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*

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

*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

Idee: Sei $a = z_n b^n + \ldots + z_1 b^1 + z_0 =$
$= (z_n b^{n-1} + \ldots + z_1) b + z_0$.
Wegen $0 \leq z_0 < b$ ist $z_0$ der Rest von $a$ nach Division durch $b$ und $m := z_n b^{n-1} + \ldots + z_1$ der ganzzahlige Quotient.

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 $i + 1$.

Bestimme die Zifferndarstellung zur Basis 2 der Anzahl der Elemente der folgenden Menge:

$$\{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s\}$$

$ab\ \ cd\ \ ef\ \ gh\ \ ij\ \ kl\ \ mn\ \ op\ \ qr\ \ \mathbf{s}$ : nullte Ziffer 1

Betrachte $\{ab, cd, ef, gh, ij, kl, mn, op, qr\}$

$abcd\ efgh\ ijkl\ \ mnop\ \ \mathbf{qr}$: erste Ziffer 1

Betrachte $\{abcd, efgh, ijkl, mnop\}$

$abcdefgh\ \ ijklmnop$ : zweite Ziffer 0

Betrachte $\{abcdefhgh, ijklmnop\}$

$abcdefhghijklmnop$ : dritte Ziffer 0

Betrachte $\{abcdefhghijklmnop\}$

... : vierte Ziffer 1

Zifferndarstellung zur Basis 2:
$10011\ (= 2^4 + 2 + 1)$

## Polynomfunktionen, Polynome

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

Wir schreiben für $f$ 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 dann $\mathbb{Q}[x]$.

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

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

gelten die gleichen Rechenregeln wie für die Addition und Multiplikation von ganzen Zahlen.

Die Rolle der Ordnung $\leq$ auf $\mathbb{Z}$ wird (in gewisser Hinsicht) von der durch den Grad bestimmten Teilordnung übernommen.

## Division mit Rest von Polynomen

**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*

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

$m$ *. . . polynomialer Quotient von* $a$ *und* $b$
$r$ *. . . 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*

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

**Beispiel:** Seien

$a := x^4+2x^3-2x^2+x-1$ und $b := x^2-2$.

Wir berechnen mit dem oben angegebenen Verfahren Polynome $m$ und $r$ mit
$a = m \cdot b + r$ und
($r = 0$ oder $grad(r) < grad(b) = 2$).
Dabei beginnen wir mit $r := a$ und schreiben die Zwischenrechnungen platzsparend untereinander.

$$\begin{array}{llllll} \mathbf{x^4} & +2x^3 & -2x^2 & +x & -1 & = (x^2+2x)b + r \\ -x^4 & & +2x^2 & & & \\ \hline & \mathbf{+2x^3} & & +x & -1 & \\ & -2x^3 & & +4x & & \\ \hline & & & \mathbf{+5x} & -1 & =: r \end{array}$$

Also ist $m = x^2 + 2x$ und $r = 5x - 1$.

## Der größte gemeinsame Teiler

Seien $a, b, c$ ganze Zahlen bzw. 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 ganzen Zahlen bzw. Polynomen ist die größte ganze Zahl, die beide teilt bzw. das normierte Polynom größten Grades, das beide teilt.

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

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

**Satz 4.** (Euklidischer Algorithmus ) *Mit dem folgenden Verfahren kann der größte gemeinsame Teiler von $a$ und $b$ berechnet werden:*

- *Falls $a, b$ ganze Zahlen sind:*
  *Ersetze $a$ und $b$ durch $|a|$ und $|b|$ .*
  *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 $ggT(a, b)$.*

- *Falls $a, b$ Polynome sind:*
  *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 des anderen ist, dann ist es (nach Division durch den Leitkoeffizienten) der $ggT(a, b)$.*

**Beispiel 5.** Mit Maple 11:

```
> 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.

**Beispiel 6.** Mit Maple 11:

```
> 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);
```

$$2x + 3$$

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

$$x^3 - 3x^2 + x - 3$$

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

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

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.

## 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 $a$.

**Satz 7.** *Die Anzahl der Nullstellen von $a$ in $\mathbb{C}$ ist*

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

**Beispiel 8.** Mit Maple 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)-degree(gcd(a,diff(a,x)),x);
```

$$6$$

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

## Ganzzahlige bzw. polynomiale lineare Gleichungen

**Satz 9.** *Es seien $a, b$ positive ganze Zahlen bzw. Polynome, beide $\neq 0$. Es gibt ganze Zahlen bzw. Polynome $u, v$ so, dass*

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

*ist. Diese können mit dem folgenden Verfahren (Erweiterter Euklid. 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 $B_1$ nicht Teiler von $A_1$ ist, berechne den ganzzahligen bzw. polynomialen Quotienten $m$ von $A_1$ und $B_1$ und setze $C := B$, $B := A - m \cdot C$ und $A := C$.*

- *Wenn $B_1$ Teiler von $A_1$ ist, dann ist $u := B_2$ und $v := B_3$ bzw. $u := lk(B_1)^{-1} \cdot B_2$ und $v := lk(B_1)^{-1} \cdot B_3$.*

**Satz 10.** *Seien $a, b, c$ ganze Zahlen bzw. Polynome, alle $\neq 0$.*
*Dann gibt es genau dann ganze Zahlen bzw. Polynome $u, v$ mit*

$$a \cdot u + b \cdot v = c,$$

*wenn $ggT(a, b)$ ein Teiler von $c$ ist.*

**Beispiel 11.** Berechne Zahlen $u, v$ so, dass

$$u \cdot 187 + v \cdot 102 = 34$$

ist!

Mit Maple 11:

```
> 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;
```

$$v := 4$$

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

## Restklassenringe

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

$a +_n b :=$ Rest von $a + b$ nach Division durch $n$

und der Multiplikation

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

heißt „Restklassenring $\mathbb{Z}$ modulo $n$“.

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

Falls $ggT(a, n) = 1$ ist:
$u \cdot a + v \cdot n = 1$, $u = m \cdot n + r$, $0 \leq r < n$
$r \cdot a + (v + m \cdot a) \cdot n = 1$, also $r \cdot_n a = 1$.

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

Anwendung der Restklassenringe: zum „schnellen Rechnen“

## Rechnen mit Restklassen von Polynomen

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

$a +_h b :=$ Rest von $a + b$ nach Division durch $h$

und der Multiplikation

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

heißt „Restklassenring $\mathbb{Q}[x]$ modulo $h$ “.

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

Falls $ggT(a, h) = 1$ ist:
$u \cdot a + v \cdot h = 1$ (Erw. Euklid. Algorithmus),
$u = m \cdot h + r,\ r = 0$ oder $grad(r) < grad(h)$,
$r \cdot a + (v + m \cdot a) \cdot h = 1$, also $r \cdot_h a = 1$.

Falls $h$ ein irreduzibles Polynom ist, ist $ggT(a, h) = 1$ für alle $a$ mit $grad(a) < grad(h)$, also ist dann $\mathbb{Q}[x]/h$ ein Körper. Das Polynom $h$ hat in diesem Körper eine Nullstelle, und zwar $x$.

**Beispiel 12.** Mit Maple 11:

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 berechnen das zu $a$ in $\mathbb{Q}[x]/h$ inverse Element.

```
> 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

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