Algebra und Geometrie in der Schule

Wintersemester 2015/16

Kap. 1: Rechnen mit ganzen und rationalen Zahlen

Ganze und Rationale Zahlen im Lehrplan der AHS

1. - 4. Klasse: „Arbeiten mit Zahlen und Maßen“
5. Klasse: „Zahlen und Rechengesetze“

1. Klasse: $\mathbb{N}, +, \cdot$, Division mit Rest, $-$ (wenn möglich);
   $\mathbb{Q}_{\geq 0}, +, \cdot, :, -$ (wenn möglich);
   Darstellung von rationalen Zahlen durch Zähler und Nenner oder durch Dezimalziffern (wenn möglich);
   Rechenregeln für $\mathbb{Q}_{\geq 0}$.
2. Klasse: Vertiefung 1. Klasse, weiters: Prozentrechnung, Teilbarkeitsregeln.
3. Klasse: $(\mathbb{Q}, +, -, \cdot, :, \leq)$, Rechenregeln, Potenzschreibweise.
4. Klasse: Zahlenverständnis vertiefen;
   Beispiele für Zahlen, die nicht rational sind, Näherungswerte dafür.
5. Klasse: Reflektieren über das Erweitern von Zahlenmengen,
   $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{Q}[a]$, Darstellen von Zahlen im dekadischen und einem nichtdekadischen Zahlensystem

Ganze und Rationale Zahlen im Lehrplan der HTL

1. Jahrgang: „Die Schülerinnen und Schüler kennen den Aufbau des Zahlensystems und können die Erweiterung der Zahlenbereiche argumentieren“; Dezimalsystem, Dualzahlen.

4. und 5. Jahrgang (z.b. Fachrichtung Informatik): Algebraische und zahlentheoretische Grundlagen der Codierung und der Chiffrierung.

Unterteilung von Kapitel 1

1.1 Natürliche Zahlen und Zifferndarstellung

Wiederholung:

- Was sind natürliche Zahlen?
- Division mit Rest (als mehrfache Subtraktion)
- Zifferndarstellung einer Zahl zur Basis $b \geq 2$

Darstellung von Zahlen durch Ziffern, Vorschlag für den Schulunterricht

Um Zahlen anzuschreiben, wählen wir Zeichen für die Zahlen Null, Eins, Zwei, Drei, Vier, Fünf, Sechs, Sieben, Acht, Neun und zwar: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. Diese Zeichen heißen *Ziffern*.

Für Zehn schreiben wir 10, für Zehn mal Zehn 100 (und sagen: Hundert), für Zehn mal Zehn mal Zehn 1000 (und sagen: Tausend), für Zehn mal Zehn mal Zehn mal Zehn 10000 (und sagen: Zehntausend).

Wenn wir Ziffern nebeneinander schreiben, zum Beispiel 3774 oder 49, dann meinen wir damit die Zahl $3 \cdot 1000 + 7 \cdot 100 + 7 \cdot 10 + 4$ oder $4 \cdot 10 + 9$. Die Worte für Zahlen werden entsprechend dieser Schreibweise gebildet: Für 3774 sagen wir drei mal Tausend und sieben mal Hundert und sieben mal Zehn und Vier oder kurz *dreitausendsiebenhundertvierundsiebzig*. Beachte: Beim „abgekürzten“ Aussprechen der Zahlwörter wird in der deutschen Sprache die Reihenfolge der letzten zwei Ziffern vertauscht! (In anderen Sprachen, zum Beispiel im Italienischen oder Englischen ist das nicht so).

Dabei ist es nicht nur wichtig, *welche Ziffern* wir anschreiben, sondern auch, in *welcher Reihenfolge* sie angeschrieben werden. Zum Beispiel kann man mit den drei Ziffern $1, 2, 3$ die sechs verschiedenen Zahlen 123, 132, 213, 231, 312, 321 anschreiben.

Die kleinsten Zahlen mit einer bzw. zwei bzw. drei Ziffern sind 0 bzw. 10 bzw. 100, die größten Zahlen mit einer bzw. zwei bzw. drei Ziffern sind 9 bzw. 99 bzw. 999.

Wiederholung: Addition von Zahlen in Zifferndarstellung

Division mit Rest für natürliche Zahlen, die in Zifferndarstellung gegeben sind

Wenn die Zahl a viel größer als b ist, ist der Divisionsalgorithmus (mehrfaches Subtrahieren) sehr langwierig. Wenn diese zwei Zahlen aber in Zifferndarstellung gegeben sind, kann man diese Zusatzinformation benutzen, um den Divisionsalgorithmus zu verbessern.

Die Idee stelle ich hier an einem Beispiel dar:
Wenn $a = 2014$ und $b = 7$ ist, dividiert man zunächst 20 mit Rest durch 7, subtrahiert also 7 zweimal und erhält $20 = 2 \cdot 7 + 6$.
Daraus schließt man $2000 = 200 \cdot 7 + 600$ und $2014 = 200 \cdot 7 + 614$ (also hat man dank der Zifferndarstellung statt 200 Subtraktionen nur 2 ausführen müssen).
Der Rest von 2014 nach Division durch 7 ist derselbe wie der von 614 nach Division durch 7 und der ganzzahlige Quotient von 2014 und 7 ist die Summe von 200 und dem ganzzahligen Quotienten von 614 und 7.
Man muss jetzt noch 614 mit Rest durch 7 dividieren, dazu geht man wieder gleich vor wie oben: $60 = 8 \cdot 7 + 4$, also ist $600 = 80 \cdot 7 + 40$, somit $614 = 80 \cdot 7 + 54$ und $2014 = 280 \cdot 7 + 54$.
Da 54 größer als 7 ist, ist noch ein weiteres „Durchlaufen der Schleife“ nötig: $54 = 7 \cdot 7 + 5$.
Nun sind wir fertig: Der ganzzahlige Quotient von 2014 nach Division durch 7 ist $287 = 200 + 80 + 7$, der Rest ist 5.
Durch Ausnutzen der Zifferndarstellung der zwei Zahlen mussten wir anstatt 287 Subtraktionen nur $2+8+7 = 17$ Subtraktionen ausführen.

Verbessertes Verfahren zur Division mit Rest für Zahlen in Zifferndarstellung (hier zur Basis 10, für andere Basen geht es aber genauso):
Zerlege $a = c_k \cdot 10^k + d_k$ so, dass $d_k < 10^k$ und $c_k < 10 \cdot b$ ist (im Beispiel: $2014 = 20 \cdot 10^2 + 14$, $14 < 10^2$, $20 < 10 \cdot 7$).
Dividiere c_k mit Rest durch b, also: $c_k = m_k \cdot b + r_k$ und $0 \leq r_k < b$.
Nach Voraussetzung an c_k ist $0 \leq m_k < 10$, es sind für diese Division mit Rest höchstens 9 Subtraktionen erforderlich. (Anstatt diese Subtraktionen auszuführen, kann man auch versuchen, den ganzzahligen Quotienten $0 \leq m_k \leq 9$ zu erraten und dann das Produkt $m_k \cdot b$ von c subtrahieren. Ist die Differenz kleiner als b und nicht negativ, dann hat man richtig geraten, sonst muss man die erste „Hypothese“ revidieren).
Solange k nicht 0 ist: Ersetze nun a durch $a - m_k \cdot b \cdot 10^k$ und k durch $k - 1$ und führe das obige noch einmal aus, erhalte $0 \leq m_{k-1} < 10$ und $0 \leq r_{k-1} < b$.
Der ganzzahlige Quotient ist dann $\sum_{i=0}^{k} m_i \cdot 10^i$, der Rest ist r_0.

Schreibt man die notwendigen Rechnungen in platzsparender Form an, erhält man das im Schulunterricht vermittelte Verfahren.

Wichtig ist: Bei diesem Verfahren zur Division mit Rest von natürlichen Zahlen, deren Zifferndarstellung bekannt ist, werden beliebige Divisionen mit Rest auf mehrere Divisionen mit Rest zurückgeführt, deren *ganzzahliger Quotient mit nur einer Ziffer darstellbar ist* (bei Dezimalziffern ist der ganzzahlige Quotient also eine natürlich Zahl, die kleiner als 10 ist).

Literatur:

Anghileri, J.: A study of progression in written calculation strategies for division. In: Support for Learning, 1/2001, S. 363-381.

Treffers, A.: Fortschreitende Schematisierung, ein natrlicher Weg zur schriftlichen Multiplikation und Division im 3. und 4. Schuljahr. In: mathematik lehren, 1/1983, S. 16-20

Pöll, J.: Die Division mit Rest in der Primarstufe. Diplomarbeit, Universität Innsbruck, 2014.

Schüler/innen müssen daher für das allgemeine Verfahren das Folgende wissen bzw. einüben:

- Die Zifferndarstellung (zur Basis 10) des 10^k-fachen einer Zahl erhält man, indem man an die ursprüngliche Zifferndarstellung k Nullen „anhängt“.
- An Hand der Dezimalziffern zweier Zahlen kann man leicht feststellen, ob die erste Zahl kleiner als die zehnfache zweite Zahl ist ($x < 10 \cdot y$?).
- Das Verfahren zur Subtraktion von Zahlen in Zifferndarstellung.
- Das Verfahren zur Division mit Rest im Fall, dass der ganzzahlige Quotient kleiner als 10 ist („Dividieren mit Rest mit einstelligem Quotienten“).

Lehrplan Volksschule, 2012:
Dritte Schulstufe: Dividieren durch einstelligen Divisor (ohne und mit Rest)
Vierte Schulstufe: Dividieren durch ein- und zweistelligen Divisor (ohne und mit Rest)

In der Sekundarstufe 2 wird auch die Zifferndarstellung zur Basis 2 betrachtet. Das Verfahren zur Division mit Rest für Zahlen in Binärdarstellung läuft genauso ab, man muss nur 10^k durch 2^k usw. ersetzen. In diesem Fall wird das Verfahren sogar besonders einfach, weil die Division mit Rest auf *eine* Subtraktion reduziert wird, wenn der ganzzahlige Quotient einziffrig (also 0 oder 1) ist.

1.2 Rationale Zahlen

Im Laufe der Schulzeit verändert sich mehrfach das, was wir mit dem Wort „Zahl“ bezeichnen. Unser Zahlenbereich wird schrittweise erweitert. Der Anlass für die Erweiterung eines Zahlenbereichs ist immer eine Aufgabe, die „eigentlich eine Lösung haben sollte“, aber im bekannten Zahlenbereich nicht lösbar ist. In der folgenden Tabelle sind einige Aufgaben, die Zahlenbereichserweiterungen motivieren, zusammengestellt.

Zahlenbereichserweiterung	**Motivation dafür z.B. durch die Aufgabe:** Finde eine Zahl z so, dass
$\mathbb{N} \subseteq \mathbb{Z}$	$3 + z = 2$
$\mathbb{Z} \subseteq \mathbb{Q}$	$3 \cdot z = 2$
$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[n]{t}]$ $(n \in \mathbb{N}_{\geq 2},\ t \in \mathbb{Q})$	$z^n = t$
$\mathbb{Q} \subseteq \mathbb{R}$	$z = \lim_{n\to\infty} t_n \quad (t_n \in \mathbb{Q})$
$\mathbb{R} \subseteq \mathbb{C}$	$z^2 = -1$

„Erweitere den Zahlenbereich K (mit $+$ und $\cdot$) zum Zahlenbereich L (mit $+$ und $\cdot$)“ (um eine gegebene Aufgabe zu lösen) heißt

- L als Menge, die K enthält, angeben,
- die Rechenoperationen $+$ und $\cdot$ auf K zu Rechenoperationen auf L erweitern,

und zwar so, dass

- der „Rechenkomfort“ erhalten bleibt, d.h. alle Rechenregeln für $+$ und $\cdot$ in K sollen auch in L gelten (insbesondere: wenn K ein Körper ist, dann soll L auch ein Körper sein),
- die gegebene Aufgabe eine Lösung in L hat
  und
- L „möglichst klein“ ist.

Zur Vorgangsweise: Beginn mit $(\mathbb{N}, +, \cdot)$.
Zwei mögliche Strategien:

- *Konstruiere sukzessive* $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$
- Finde „Modell“ für $(\mathbb{R}, +, \cdot)$ (zum Beispiel *Zahlengerade* mit $+$ und $\cdot$), definiere dann $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}]$, ... als Teilmengen mit induzierten Rechenoperationen, konstruiere schließlich $\mathbb{R} \subseteq \mathbb{C}$. (Beginn mit Modell für $\mathbb{C}$ wäre auch möglich).

Wiederholung:

- Konstruktion der Erweiterung $\mathbb{N} \subseteq \mathbb{Q}_{\geq 0}$.
- Zifferndarstellung von gewissen Bruchzahlen

1.3 Teilbarkeit

Wiederholung: Teiler, Vielfaches

Der größte gemeinsame Teiler von zwei Zahlen

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

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

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 $ggT(a, b)$.

Wiederholung: Teilbarkeitsregeln

1.4 Primzahlen und Verschlüsselung mit öffentlichem Schlüssel

Wiederholung:

- Primzahlen
- Eindeutige Zerlegung von positiven ganzen Zahlen in Primfaktoren
- Es gibt unendlich viele Primzahlen
- Der erweiterte Euklidische Algorithmus

- Der Restklassenring $\mathbb{Z}_n$
- Der „kleine Satz von Fermat“
- Kongruenzensysteme (chinesischer Restsatz)

RSA-Verfahren

- Der Empfänger gibt zwei sehr große natürliche Zahlen n und e öffentlich bekannt.
- Der Sender will dem Empfänger die Zahl a verschlüsselt mitteilen.
- Dazu berechnet er die Zahl b, den Rest von a^e nach Division durch n.
$$b = a^e \; mod \, n$$
- Der Empfänger erhält b und berechnet für eine geeignete Zahl d den Rest von b^d nach Division durch n und erhält a !
$$b^d \; mod \; n = a$$

Was weiß nur der Empfänger?

- Er kennt Primzahlen p und q mit
$$n = p \cdot q \, .$$
- Er hat e so gewählt, dass
$$ggT(e, (p-1) \cdot (q-1)) = 1$$
ist.
- Er berechnet Zahlen c und d so, dass
$$m \cdot c + e \cdot d = 1$$
ist, wobei $m := (p-1) \cdot (q-1)$ ist.

3 Fragen:

1. Die Zahl n ist bekannt. Warum kann nicht jede/r ihre Primfaktoren p und q berechnen?

2. Wie werden die ganzen Zahlen c und d
(mit $(p-1) \cdot (q-1) \cdot c + e \cdot d = 1$) berechnet?
Oder: Wie löst man eine lineare Gleichung mit zwei Unbekannten ganzzahlig?

3. Warum ist für alle ganzen Zahlen a der Rest von
$$a^{e \cdot d} = a^{1-(p-1) \cdot (q-1) \cdot c} = a \cdot (a^{(p-1) \cdot (q-1)})^{-c}$$
nach Division mit Rest durch $n = p \cdot q$ gleich a ?

2009: Faktorisierung der Zahl RSA-768 mit 232 Dezimalziffern bzw. 768 Binärziffern
Rechenzeit von mehreren hundert Computern: zweieinhalb Jahre

RSA-1024 =
135066410865995223349603216278805969938
881475605667027524485143851526510604859
533833940287150571909441798207282164471
551373680419703964191743046496589274256
239341020864383202110372958725762358509
643110564073501508187510676594629205563
685529475213500852879416377328533906109
750544334999811150056977236890927563

309 Dezimalziffern, 1024 Binärziffern, mit heutigen Methoden nicht in diesem Jahrhundert faktorisierbar

Bemerkung: „Euklidischer Algorithmus versus Produkt der gemeinsamen Primfaktoren“:

- „Theorie“ einfacher: EA
- Historisch: EA älter
- Einfach zu programmieren: EA
- Rechnerische Effizienz: EA (!!!!)
- Vermittelt Problemlösestrategie: EA

Methode des Produkts der gemeinsamen Primfaktoren legt „falsche Fährte“ , erschwert Verständnis z.B. des RSA-Verfahrens.