Modulo-Rechnungen und Restklassen

Ein „Stück“ Zahlentheorie

Stand: 9. Februar 2019

Datei Nr. 55010

FRIEDRICH W. BUCKEL

INTERNETBIBLIOTHEK FÜR SCHULMATHEMATIK

www.mathe-cd.de

Vorwort

Aus der Teilbarkeitslehre ganzer Zahlen heraus kann man Untersuchungen über die verschiedenen Möglichkeiten an Divisionsresten anstellen. Vertieft man dies, kommt man zu den sogenannten Modulo-Rechnungen und den Restklassen.

Dies führt – wie so oft in der Mathematik – sehr in die Tiefe, wenn man hartnäckig weiter forscht.

Ich versuche hier die Anfänge möglichst anschaulich darzustellen und vermeide auch große „Tiefen“, damit der Text für Gymnasiasten und Studienanfänger noch lesbar bleibt.

Inhalt

1 Rechnen mit Resten - Modulo-Rechnungen

1.1 Einführende Betrachtung

Beispiel 1 Wenn man eine natürliche Zahl ***durch 5 dividiert***, kann es genau 5 Reste geben, nämlich 0 (wenn die Zahl durch 5 teilbar ist), oder Rest 1, Rest 2, Rest 3, Rest 4. Rest 5 ist nicht möglich, denn dann wurde falsch dividiert: Dann gibt es Rest 0.

Zwei natürliche Zahlen a und b heißt man ***kongruent modulo 5,*** wenn die Differenz a – b ein Vielfaches von 5 ist.

Diese Definition klingt zunächst etwas abstrakt. So aber wird sie in der Literatur meist genannt. Man kann sie natürlich auch einfacher formulieren:

Zwei natürliche Zahlen a und b heißt man ***kongruent modulo 5***, wenn sie bei Division durch 5 den gleichen Rest ergeben.

Man kann sich schnell klar machen, dass beide Definitionen dasselbe meinen.
Ich wähle als Beispielzahlen a = 38 und b = 23.

(a) Zuerst beweise ich, dass bei gleichem Rest a – b durch 5 teilbar ist:
Bei Division durch 5 ergeben beide Zahlen den Rest 3, sind also nach der zweiten Definition kongruent modulo 5.
Nun schauen wir uns ihre Differenz an: a – b = 15 ist ein Vielfaches von 5. Alles klar!

Das verallgemeinern wir nun und verwenden zwei Zahlen mit dem gleichen Rest r:

$a = u \cdot 5 + r$ hat den Rest r (u und v seien so gewählt, dass $0 \le r \le 4$ ist)

$b = v \cdot 5 + r$ hat auch den Rest r.

Dann folgt für die Differenz:

$$a - b = (u \cdot 5 + r) - (v \cdot 5 + r) = u \cdot 5 - v \cdot 5 = (u - v) \cdot 5$$

d. h. a – b ist ein Vielfaches von 5.

(b) Nun zeige ich, dass zwei Zahlen a, b deren Differenz ein Vielfaches von 5 ist, auch den gleichen Fünferrest haben:

Es sei a – b ein Vielfaches von 5, dann ist $a - b = k \cdot 5$.

Für a und b gibt es eine Restdarstellung: $a = u \cdot 5 + r$ und $b = v \cdot 5 + s$

Daraus wird die Differenz berechnet: $a - b = (u \cdot 5 + r) - (v \cdot 5 + s) = (u - v) \cdot 5 + (r - s)$

Weil wir aber andererseits bereits wissen: $a - b = k \cdot 5$, dann muss $r - s = 0$ sein, also r = s.

Schreibweise: $a \equiv b$ **modulo m** **Manche schreiben** $a = b \pmod m$

heißt also:
1. a und b haben bei Division durch m den gleichen Rest,
2. a – b ist ein Vielfaches von m.

Beispiel 2: Teilbarkeit durch 7

21 hat bei Division durch 7 den Rest 0: $21 \equiv 0 \mod 7$

70 hat bei Division durch 7 den Rest 0: $70 \equiv 0 \mod 7$

21 und 70 haben bei Division durch 7 den gleichen Rest: $21 \equiv 70 \mod 7$

Diese Relation ist symmetrisch, denn man kann auch sagen:

70 und 21 haben bei Division durch 7 den gleichen Rest: $70 \equiv 21 \mod 7$

Ferner gilt: $15 \equiv 50 \mod 7$, denn 15 : 7 = 2 Rest 1, 50 : 7 = 7 Rest 1

Man kann natürlich auch mit negativen ganzen Zahlen eine Modulo-Arithmetik betreiben:

Beispiel 3: Ich zeige zwei Divisionsrechnungen. *Entscheiden Sie, welche man für eine modulo-Aussage verwenden kann:*

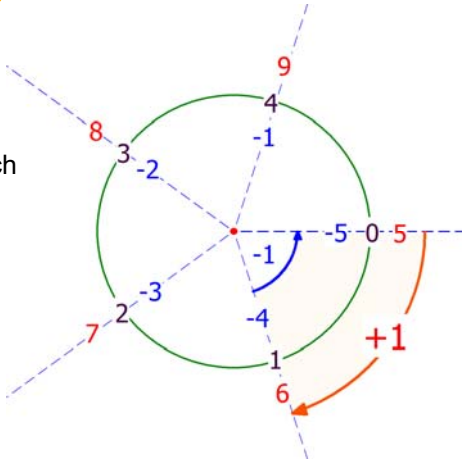
-8 : 5 = -1 Rest -3, denn $5 \cdot (-1) + (-3) = -8$

oder -8 : 5 = -2 Rest 2, denn $5 \cdot (-2) + 2 = -8$

Dazu gibt es eine schöne Darstellung, die das Arbeiten mit modulo gut erklärt:

Dieses „Modulo-Rad“ gehört zu modulo 5.

Auf der Kreislinie stehen die Reste 0 bis 4. Addiert man fortgesetzt **+1** kommt man zu jeweils nächsten Zahl.
Ist man bei 4 angekommen, dann führt **+1** zur Zahl 5, die jedoch bereits wieder den Divisionsrest 0 hat. Sie steht daher auf demselben Radius wie die Zahl 0, die ja auch Rest 0 hat.
Wenn man weiterhin **+1** rechnet, erreicht man 6 bis 9.
6 hat Rest 1 und steht daher auf dem gleichen Radius wie 1.
Von 9 aus gelangt man mittels **+1** zu 10. Diese Zahl hat den Rest 0, weshalb 10 rechts von der 5 stehen sollte, usw.



Man kann sich auf diesem „Modulorad“ auch rückwärts bewegen, also z.B. von 2 aus durch **-1** nach 1, dann nach 0 und weiter nach -1. Diese Zahl steht auf dem Radius der Zahl 4, also nicht wie manche erwarten würden auf dem Radius der Zahl 1. Begründung: Den Rest 0 haben alle Vielfachen von 5. Geht man von -5 aus und addiert den Rest 4, dann kommt man zu -1.

Nun ist es einfach, die oben gestellte Frage zu beantworten: Wo muss in unserem Modulorad die Zahl -8 stehen. Zählt man von -5 aus um 3 zurück, gelangt man zum Radius der Zahl 2.
Die zugehörige Rechnung sieht so aus:

-8 : 5 = -2 Rest 2

Denn die zugelassenen Reste sind ja positiv, also scheidet die Division aus, die zum Rest – 3 führt.

1.2 Restklassen

Man kann alle Zahlen mit demselben Rest zu einer Restklasse zusammenfassen.
Alle Zahlen einer Restklasse stehen im Modulorad auf demselben Radius.

Die meist verwendete Schreibweise z.B. für die ***Restklassen modulo 5*** sieht so aus:

$\overline{0} = \{0, \pm 5, \pm 10, ...\} = \{x \mid x = 5 \cdot z,\ z \in \mathbb{Z}\}$	Alle Zahlen mit Rest 0.
$\overline{1} = \{..., -9, -4, 1, 6, ...\} = \{x \mid x = 5z + 1, z \in \mathbb{Z}\}$	Alle Zahlen mit Rest 1.
$\overline{2} = \{..., -8, -3, 2, 7, ...\} = \{x \mid x = 5z + 2, z \in \mathbb{Z}\}$	Alle Zahlen mit Rest 2.
$\overline{3} = \{..., -7, -2, 3, 8, ...\} = \{x \mid x = 5z + 3, z \in \mathbb{Z}\}$	Alle Zahlen mit Rest 3.
$\overline{4} = \{..., -6, -1, 4, 9, ...\} = \{x \mid x = 5z + 4, z \in \mathbb{Z}\}$	Alle Zahlen mit Rest 4.

Da es bei Division durch eine natürliche Zahl n genau n Reste geben kann, nämlich 0 bis n-1,
gibt es zu jeder Zahl n genau n Restklassen: $\overline{0}$, $\overline{1}$ bis $\overline{n-1}$.

Es gibt einige Regeln, wie man mit *modulo* arbeiten kann.
Diese lassen sich hervorragend mit den Restklassen und dem Modulorad klären.

Satz 1:

Voraussetzung: a, b, c, d seien $\in \mathbb{Z}$, $m \in \mathbb{N} \setminus 1$.

Ferner sollen a und b derselben Restklasse angehören.

Mit anderen Worten: Es sei $a \equiv b \mod m$ und $c \equiv d \mod m$.

Dann gelten folgende Aussagen (a, b, e und f werden auf der nächsten Seite bewiesen):

(a) $a + c \equiv b + c \mod m$.

Das heißt, dass dann auch a+c und b+c derselben Klasse angehören.

(b) $a + c \equiv b + d \mod m$.

Das heißt, dass dann auch a+c und b+d derselben Klasse angehören.

(c) $a - c \equiv b - c \mod m$.

Das heißt, dass dann auch a-c und b-c derselben Klasse angehören.

(d) $a - c \equiv b - d \mod m$.

Das heißt, dass dann auch a-c und b-d derselben Klasse angehören.

(e) $a \cdot c \equiv b \cdot c \mod m$.

Das heißt, dass dann auch ac und bc derselben Klasse angehören.

(f) $a \cdot c \equiv b \cdot d \mod m$.

Das heißt, dass dann auch ac und bd derselben Klasse angehören.

(g) $a^k \equiv b^k \mod m$ für alle $k \in \mathbb{N}_0$

Das heißt, dass dann auch a^k und b^k derselben Klasse angehören.

Achtung: (g) gilt nicht für die Exponenten, d. h. $r \equiv s \mod m \Rightarrow a^r \equiv a^s \mod m$ **gilt nicht.**

Beispiel: $1 \equiv 6 \mod 5$. Aber $2^1 \equiv 2^6 \mod 5$ ist falsch, dann $2^6 = 64 \equiv 4 \mod 5$.

Beweis zu (a):

Vorausgesetzt ist $a \equiv b \mod m$. Also gehören a und b derselben Restklasse an.

Also sind sie auf dem Modulorad am gleichen Radius angeordnet.

Addiert man die Zahl c, bewegt man sich um c Einheiten weiter (im Uhrzeigersinn), wobei eine Einheit dem Winkel $\frac{360}{m}$ Grad entspricht. Dies gilt für a genauso wie für b, also liegen die Ergebnisse a+c und b+c in der gleichen Restklasse.

Man kann dies auch algebraisch beweisen:

$a \equiv b \mod m$ bedeutet: $a - b = k \cdot m$

Nun addiere ich die Nullsumme (+c-c) auf diese Weise:

$a - b = a + c - b - c$ und erhalte:

$a - b = (a + c) - (b + c)$

Und da a-b nach Voraussetzung ein Vielfaches von m ist, gilt dasselbe für (a+c) – (b+c), was zu beweisen war.

Beweis zu (b):

Nach Voraussetzung ist $a \equiv b \mod m$, also ist $a - b = k \cdot m$ (1).

Ferner sei $c \equiv d \mod m$, also ist $c - d = h \cdot m$ (2).

Addiert man (1) + (2), erhält man: $(a - b) + (c - d) = km + hm$

Umordnen liefert: $(a + c) - (b + d) = (k + h)m$

D. h. dass $(a + c) - (b + d)$ ein Vielfaches von m ist

Also gilt $(a + c) \equiv (b + d) \mod m$, was zu beweisen war.

Beweis zu (e):

Nach Voraussetzung ist $a \equiv b \mod m$, also ist $a - b = k \cdot m$ (1).

Die Behauptung lautet: $ac \equiv bc \mod m$, also $ac - bc = hm$. (2)

Dazu multiplizierte man (1) mit c: $(a - b) \cdot c = c \cdot km$

Umordnen liefert: $ac - bc = (ck) \cdot m$

was genau der Gleichung (2) entspricht mit h = ck.

Beweis zu (f):

Nach Voraussetzung ist $a \equiv b \mod m$, also ist $a - b = k \cdot m$ (1).

Ferner sei $c \equiv d \mod m$, also ist $c - d = h \cdot m$ (2).

Die Behauptung lautet: $ac \equiv bd \mod m$, also $ac - bd = u \cdot m$ (3)

Aus (1) folgt durch Multiplikation mit c: $ac - bc = ck \cdot m$ (4)

Aus (2) folgt durch Multiplikation mit b: $bc - bd = bh \cdot m$ (5)

(4) + (5) ergibt: $ac - bc + bc - bd = ck \cdot m + bh \cdot m$

d. h. $ac - bd = (ck + bh) \cdot m$ (6)

(6) entspricht der Behauptung (3) mit $u = ck + bh$, was zu beweisen war.

1.3 Teilbarkeitsregel für die Division durch 9

Eine bekannte Teilbarkeitsregel gilt für die Division durch 9. Sie lautet:

(1) Die Quersumme einer Zahl hinterlässt bei Division durch 9 denselben Rest wie die Zahl selbst.

Ein Spezialfall davon ist diese Regel:

(2) Ist die Quersumme einer Zahl durch 9 teilbar, dann ist es auch die Zahl selbst.

Ich beweise zuerst die Regel (2) für den Fall einer fünfstelligen Zahl z.

Es seien a, b, c, d, e die fünf Ziffern einer fünfstelligen Zahl z.
Dann ist sicher $a \neq 0$, denn sonst wäre sie ja nicht mehr fünfstellig.

Ich schreibe z so: $z = \text{"abcde"} = a \cdot 10000 + b \cdot 1000 + c \cdot 100 + d \cdot 10 + e$

Nun setzen wir voraus, dass die Quersumme $q = a + b + c + d + e$ durch 9 teilbar ist.

Nun zerlege ich: $z = 9999a + a + 999b + b + 99c + c + 9d + d + e$

und ordne neu: $z = [9999a + 999b + 99c + 9d] + (a + b + c + d + e)$

Die runden Klammern beinhalten die Quersumme, die ja nach Voraussetzung durch 9 teilbar ist, in der eckigen Klammer steht eine Summe, die offensichtlich auch durch 9 teilbar ist. Ferner weiß man dass die Summe zweier durch 9 teilbaren Zahlen auch durch 9 teilbar ist (man kann 9 ausklammern). Also ist z selbst durch 9 teilbar.

Ich beweise nun die Regel (1) für den Fall einer fünfstelligen Zahl.

Ich setze voraus, dass die Quersumme bei Division einen Rest r lässt.

Dann schreibe ich wie oben: $z = \text{"abcde"} = a \cdot 10000 + b \cdot 1000 + c \cdot 100 + d \cdot 10 + e$

und zerlege $z = 9999a + a + 999b + b + 99c + c + 9d + d + e$

und ordne um: $z = [9999a + 999b + 99c + 9d] + (a + b + c + d + e)$

Nach Voraussetzung ist ja $q = a + b + c + d + e = k \cdot 9 + r$ (Rest r!)

Dann gilt auch $z = \underbrace{[9999a + 999b + 99c + 9d] + k \cdot 9}_{\text{durch 9 teilbar}} + r$

Also hinterlässt auch z selbst den Rest r.

Ergebnis: $z \equiv q \mod 9$

Man kann diesen Beweis mühelos auf beliebig-stellige Zahlen z ausdehnen.

1.4 Fehlerkontrolle

Beispiel 1: ***Behauptung***: $259 \cdot 517 = 133803$

Nach 1.3 hat eine Zahl denselben Neunerrest wie ihre Quersumme:

$259 \equiv 16 \equiv 7 \mod 9$ wobei 7 die Quersumme von 16 ist,

$517 \equiv 13 \equiv 4 \mod 9$.

Also gilt: $259 \cdot 517 \equiv 7 \cdot 4 = 28 \equiv 1 \mod 9$

Andererseits ist $133803 \equiv 18 \equiv 0 \mod 9$.

Also kann das Ergebnis nicht stimmen.

Beispiel 2: ***Behauptung*:** $143 \cdot 5920 = 816703$

$143 \equiv 8 \mod 9$ (denn $143 = 15 \cdot 9 + 8$)

$5920 \equiv 7 \mod 9$ (denn $5920 = 567 \cdot 9 + 7$)

Also: $143 \cdot 5920 \equiv 8 \cdot 7 = 56 \equiv 2 \mod 9$ (denn $56 = 9 \cdot 6 + 2$)

Andererseits ist: $816703 \equiv 25 \equiv 7 \mod 9$.

Also kann das Ergebnis nicht stimmen.

1.5 Andere Anwendungen

1. Eine Kürzungsregel:

Voraussetzung: Es sei $ak \equiv bk \mod m$

und k sei teilerfremd zu m d. h. ggT(k,m)=1.

Dann kann man die Modulo-Gleichung durch k kürzen,

d. h. es gilt: $ak \equiv bk \mod m \Rightarrow a \equiv b \mod m.$

Beispiel 1: Es ist $35 \equiv 77 \mod 6$, denn $35 : 6 = 5$ Rest 5.

und $77 : 6 = 12$ Rest 5.

Nun haben 35 und 77 den gemeinsamen Teiler 7, und ggT(7,6)=1.

Also darf man die Modulo-Gleichung durch 7 kürzen:

$35 \equiv 77 \mod 6 \Rightarrow 5 \equiv 11 \mod 6$, was eine wahre Aussage ist.

Beispiel 2: Es ist $10 \equiv 4 \mod 6$, denn $10 : 6 = 1$ Rest 4.

Nun haben 10 und 4 den gemeinsamen Teiler 2.

Wenn ich diese Modulo-Gleichung durch 2 kürze, entsteht:

$10 \equiv 4 \mod 6 \Rightarrow 5 \equiv 2 \mod 6$, was eine falsche Aussage ist.

Dieser Fehler entsteht, weil $ggT(2,6) \neq 1$ ist, 2 und 6 haben den gemeinsamen Teiler 2, und dann ist Kürzen nicht erlaubt. In manchen Fällen mag das gut gehen, aber nicht immer.

Etwa folgt aus $15 \equiv 33 \mod 6$ durch Kürzen durch 3 die wahre Aussage $5 \equiv 11 \mod 6$, obwohl 6 und 3 nicht teilerfremd sind.

Beweis der Kürzungsregel:

Nach Voraussetzung sollen die beiden Seiten einer Modulo-Gleichung einen gemeinsamen Teiler k besitzen. Dann kann man diese Gleichung so darstellen: $a \cdot k \equiv b \cdot k \mod m$.

Das heißt aber, dass m ein Teiler von $(ak - bk)$, also von $(a - b) \cdot k$ ist.

Ferner sollen k und m teilerfremd sein, also kann m kein Teiler von k sein. Folglich muss m ein Teiler von (a - b) sein. Und das wiederum heißt: $a \equiv b \mod m$.

2. Eine merkwürdige Regel

Unter 5 verschiedenen ganzen Zahlen gibt es immer drei, deren Summe durch 3 teilbar ist.

Beispiel: $A = \{2,3,5,-1,-7\}$ $2+5+(-1)=6$ ist durch 3 teilbar.

$B = \{-2,-5,0,3,11\}$ $(-2)+0+11=9$ ist durch 3 teilbar.

Beweis:

Ich bezeichne die fünf Zahlen mit a, b, c, d und e. Alle sind kongruent zu 0, 1 oder 2 modulo 3.
Also gibt es für diese 5 Zahlen genau drei „Schubfächer“, in denen sie liegen können.

1. Fall: Liegen drei Zahlen im gleichen Fach, ist ihre Summe kongruent zu 0, 3 oder 6, also ist ihre Summe durch 3 teilbar.

2. Fall: Tritt der 1. Fall nicht auf, d. h. liegen höchstens 2 Zahlen im gleichen Fach, dann sind folgende Verteilungen möglich

Rest 0	Rest 1	Rest 2
a, b	c, d	e

$a+c+e \equiv 3 \equiv 0 \mod 3$

Rest 0	Rest 1	Rest 2
a, b	c	d, e

$a+c+e \equiv 3 \equiv 0 \mod 3$

Rest 0	Rest 1	Rest 2
a	b, c	d, e

$a+c+e \equiv 3 \equiv 0 \mod 3$

Dadurch, dass im 2. Fall nicht alle drei in einer Restklasse liegen, muss in jeder der drei Schubfächer (Restklassen) mindestens eine der fünf Zahlen liegen.
Und deren Summe ist 0 + 1 + 2 modulo 3, was zu beweisen war.

Das war das sogenannte „Schubfachprinzip“.

2 Rechnen mit Restklassen

2.1 Addition von Restklassen

.....