Rechnen mit Kongruenzen
Arbeitsmaterial für Klasse 7

Hans-Gert Gräbe, Leipzig

Kongruenzen oder Restklassen sind ein sehr wichtiges Hilfsmittel, mit dem sich viele Überlegungen, in denen in der einen oder anderen Form Teilbarkeitsaussagen auftreten, besonders elegant formulieren lassen. Hat man einmal die grundlegenden Prinzipien dieser *Modulrechnung* verstanden, dann ist sie auch ein wichtiges Hilfsmittel zum Auffinden von Lösungen entsprechender Aufgaben.

Im weiteren sei eine ganze Zahl $m > 1$ fixiert, der *Modul*, bezüglich welcher wir Teilbarkeitsaussagen untersuchen wollen.
Wir sagen, dass zwei ganze Zahlen $a, b \in \mathbb{Z}$ *kongruent modulo* m sind, und schreiben

$$a \equiv b \pmod{m} \qquad \text{oder kurz} \qquad a \equiv b\ (m),$$

wenn a und b „bei Division durch m denselben Rest lassen“. So gilt etwa $73 \equiv 38\ (7)$, denn beide Zahlen lassen bei Division durch 7 den Rest 3. Ähnlich gilt $71 \equiv 23\ (8)$, weil beide Zahlen bei Division durch 8 den Rest 7 lassen.
Diese Definition, unter der ihr euch hoffentlich etwas vorstellen könnt, ist zwar sehr einprägsam und für positive a, b auch verständlich, aber entbehrt doch der für exakte mathematische Argumentation notwendigen Strenge. Eine dem ursprünglichen Anliegen entsprechende Aussage, die dem Anspruch an eine solche Strenge genügt, ist die Überlegung, dass zwei Zahlen bei Division durch m genau dann denselben Rest lassen, wenn deren Differenz durch m teilbar ist. Auf diese Weise verbinden wir den neuen Begriff „kongruent“ mit dem bereits bekannten Begriff der Teilbarkeit:

$$a \equiv b \pmod{m} \ :\Leftrightarrow\ m \,|\, (a - b)$$

Eine solche Beziehung zwischen zwei Zahlen (und allgemeiner mathematischen Größen) bezeichnet man auch als *Relation* und $\equiv$ als die *Kongruenzrelation*. Die Kongruenzrelation hat drei grundlegende Eigenschaften; sie ist

- reflexiv (das heißt $a \equiv a \pmod{m}$),
- transitiv (das heißt $a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$)
- und symmetrisch (das heißt $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$).

Relationen mit diesen drei Eigenschaften bezeichnet man auch als *Äquivalenzrelationen*. Wir wollen diese drei Eigenschaften hier beweisen, indem wir die jeweilige Aussage über Kongruenzen in eine solche über Teilbarkeit umformulieren und dann unser Wissen über Teilbarkeitsaussagen anwenden:

Reflexivität: Es gilt stets $a \equiv a \pmod m$, denn $m \,|\, (a-a) = 0$ (bekanntlich ist jede Zahl Teiler der Zahl 0).

Symmetrie: Wenn $a \equiv b \pmod m$ gilt, so gilt auch $b \equiv a \ (m)$: Ist m ein Teiler von $(a-b)$, so ist m auch ein Teiler von $(b-a)$.

Transitivität oder *Drittengleichheit*: Wenn $a \equiv b \ (m)$ und $b \equiv c \pmod m$ gilt, so gilt auch $a \equiv c \pmod m$: Ist m sowohl ein Teiler von $(a-b)$ als auch von $(b-c)$, so ist m auch ein Teiler von $(a-c) = (a-b) + (b-c)$.

An dieser Stelle sei daran erinnert, wie Teilbarkeit definiert ist: Eine ganze Zahl $u \in \mathbb{Z}$ heißt *Teiler* einer Zahl $v \in \mathbb{Z}$, wenn es eine dritte Zahl $t \in \mathbb{Z}$ gibt, so dass $v = u \cdot t$ gilt (z.B. gilt $3 \,|\, 12$, weil es die Zahl $t = 4$ gibt mit $3 \cdot 4 = 12$). m ist also genau dann Teiler der Zahl $(a-b)$, wenn es eine Zahl $t \in \mathbb{Z}$ mit $a - b = m \cdot t$ gibt, oder anders

$$a \equiv b \ (mod\ m) \ \Leftrightarrow \ m \,|\, (a-b) \ \Leftrightarrow \ \exists\, t \in \mathbb{Z} \ : \ a = b + m \cdot t$$

Oft ist es wichtig, zwischen diesen drei Möglichkeiten, die Kongruenzeigenschaft zu formulieren, zu wechseln. So sind etwa die drei folgenden Aussagen äquivalent:

$$z \equiv 5 \ (8) \ \Leftrightarrow \ 8 \,|\, (z-5) \ \Leftrightarrow \ \exists\, t \in \mathbb{Z} \ : \ z = 8t + 5$$

Mit Kongruenzen kann man fast genauso wie mit Gleichungen rechnen. Es gilt

$$a \equiv b \pmod m,\ c \equiv d \pmod m \ \Rightarrow \ \begin{cases} a + c \equiv b + d & \pmod m \\ a - c \equiv b - d & \pmod m \\ a \cdot c \equiv b \cdot d & \pmod m \end{cases}$$

Nur bei der Division muss man vorsichtig sein !

Wir wollen die erste Aussage beweisen: Ist $a \equiv b \pmod m$, also $m \,|\, (a-b)$, so gilt auch $a + c \equiv b + c \pmod m$, denn die Differenz $(a+c) - (b+c)$ beider Seiten ist genau $(a-b)$, also durch m teilbar. Genauso zeigen wir, dass aus $c \equiv d \pmod m$ die Kongruenz $b + c \equiv b + d \pmod m$ folgt, womit sich schließlich $a + c \equiv b + d \pmod m$ nach der Drittengleichheit ergibt.

Aufgabe 1 Beweise auch die anderen beiden Aussagen sowie die vierte wichtige Beziehung

$$a \equiv b \pmod m \ \Rightarrow \ \forall\, n \in \mathbb{N}\ a^n \equiv b^n \pmod m.$$

Wir können also in jedem *arithmetischen Ausdruck*, d.h. in einem solchen, wo die einzelnen Größen nur durch die vier Grundrechenarten verbunden sind, und in dem keine Division vorkommt, Zahlen durch andere Zahlen mit demselben Rest $\pmod m$ ersetzen, ohne dass sich der Rest des Ausdrucks ändert. Insbesondere kann man eine Zahl stets durch ihren *kleinsten nichtnegativen Rest* ersetzen, d.h. durch eine Zahl im Intervall $[0, m-1]$. Es spielen aber auch negative Reste mit kleinem Absolutbetrag (z.B. der Rest $m - 1 \equiv (-1) \pmod m$) eine wichtige Rolle.

Wir können damit Aufgaben der folgenden Art einfach lösen:

Aufgabe 2 Zeige, dass $z = 43^7 - 87^{13}$ durch 44 teilbar ist.

Zum Beweis dieser Aussage müssen wir die Zahl z zum Glück nicht ausrechnen[1], sondern nur $z \equiv 0\ (44)$ zeigen. Dazu können wir alle Summanden und Faktoren durch einfachere Zahlen ersetzen, wenn diese nur bei Division durch 44 denselben Rest lassen. Nun gilt aber $87 \equiv 43 \equiv (-1)\ (44)$ (letzteres, weil 44 ein Teiler von $(43 - (-1)) = (43 + 1)$ ist) und folglich

$$z \equiv (-1)^7 - (-1)^{13} = (-1) - (-1) = 0\ (44).$$

Beachte den Wechsel von $\equiv$ und $=$ in dieser Kette ! $\equiv$ wird verwendet, wenn die Ausdrücke links und rechts des Zeichens nur denselben Rest lassen, $=$ dagegen, wenn die Ausdrücke wirklich gleich sind.

Aufgabe 3 Auf welche 3 Ziffern endet die Zahl 2^{100} ?

Rechnet man diese 30-stellige Zahl auf einem Taschenrechner aus, so erhält man je nach Anzeige die *ersten* 8 – 12 Ziffern, aber keine Information über die *letzten* Ziffern. Informationen über diese Ziffern erhält man aber aus der Modulrechnung, denn *die letzten drei Ziffern einer Zahl sind gerade deren Rest bei Division durch 1000.* Bei den folgenden Rechnungen leistet ein Taschenrechner trotzdem gute Dienste. Wir schreiben zuerst $2^{100} = (2^{10})^{10} = 1024^{10}$ (gruppiere die 100 Faktoren 2 zu 10 Gruppen zu je 10 Faktoren) und ersetzen $1024 \equiv 24\ (1000)$. Dies liefert

$$2^{100} \equiv 24^{10} = (24^3)^3 \cdot 24\ (1000).$$

Der Taschenrechner hilft weiter: $24^3 = 13\,824 \equiv 824\ (1000)$, also

$$2^{100} \equiv 824^3 \cdot 24 = (824^2) \cdot (824 \cdot 24)\ (1000).$$

Weiter mit dem Taschenrechner: $824^2 = 678\,976 \equiv 976\ (1000)$ und $824 \cdot 24 = 19\,776 \equiv 776\ (1000)$, also

$$2^{100} \equiv 976 \cdot 776 = 757\,376 \equiv 376\ (1000).$$

Die Zahl endet also auf die drei Ziffern 376.

Natürlich ist es heute nicht schwer, Software für einen Computer zu finden, die eine solche Zahl exakt berechnet. Man erhält dann

$$2^{100} = 1\,267\,650\,600\,228\,229\,401\,496\,703\,205\,376$$

Aufgabe 4 Finde die letzten drei Ziffern der beiden Zahlen 2^{1000} und 3^{1000} !

(Antwort, zum Vergleich: 376 und 001)

Eine weitere Besonderheit des Rechnens mit Kongruenzen beruht auf der Tatsache, *dass es nur endlich viele verschiedene Klassen von Resten gibt.* Teilbarkeitsaussagen kann man deshalb oft durch eine Fallunterscheidung beweisen, wie in der folgenden Aufgabe.

Aufgabe 5 Zeige, dass eine Quadratzahl bei Division durch 4 nur den Rest 0 oder 1 lassen kann !

[1] Es gilt $z = -1635875635153002569916194 0$

Eine Quadratzahl hat immer die Gestalt a^2 mit einer natürlichen Zahl $a \in \mathbb{N}$. Da es bei ihrem Rest (*mod* 4) nur auf den Rest von a ankommt, können wir die Aussage durch vollständige Fallunterscheidung (in Tabellenform) lösen:

$a \pmod 4$	$a^2 \pmod 4$
0	0
1	1
2	$4 \equiv 0$
3	$9 \equiv 1$

Aufgabe 6 Zeige, dass die Summe zweier ungerader Quadratzahlen niemals eine Quadratzahl sein kann.

Aufgabe 7 Beweise folgende Aussage: Ist die Summe zweier Quadratzahlen durch 3 teilbar, so auch jeder der beiden Summanden.

Attribution Section

graebe (2004-09-02):
Dieses Material wurde vor einiger Zeit als Begleitmaterial für den LSGM-Korrespondenzzirkel in der Klasse 7 erstellt und nun nach den Regeln der KoSemNet-Literatursammlung aufbereitet.