Das Rechnen mit Kongruenzen. Teil 2
Arbeitsmaterial für Klasse 8

Hans-Gert Gräbe, Leipzig

Dieser Text baut auf dem Text „Rechnen mit Kongruenzen“ (graebe-04-4) auf.

Die Kürzungsregeln

Wir wollen das Arbeitsblatt „Rechnen mit Kongruenzen“ noch um zwei Rechenregeln erweitern, die das „Dividieren“ von Resten betreffen. Da Restklassen aus dem Bereich der ganzen Zahlen entstanden sind, in dem man bekanntlich Divisionen nicht uneingeschränkt ausführen kann (dazu muss man sie zu den rationalen Zahlen erweitern), ist dabei jedoch Vorsicht am Platze! Insbesondere, da Reste ja ein Ausdruck dafür sind, wie sehr die Division nicht aufgeht, wollen wir den Begriff „Division“ im Zusammenhang mit Resten gänzlich vermeiden und von *Kürzungsregeln* sprechen.

1. Kürzungsregel: Enthalten in der Kongruenz

$$a \equiv b \pmod{m}$$

die Zahlen a, b, m alle einen gemeinsamen Faktor d, d.h. lassen sie sich als $a = d \cdot a',\ b = d \cdot b',\ m = d \cdot m'$ darstellen, so gilt auch

$$a' \equiv b' \pmod{m'}.$$

2. Kürzungsregel: Enthalten in der Kongruenz

$$a \equiv b \pmod{m}$$

die Zahlen a, b einen gemeinsamen Faktor d, d.h. lassen sie sich als $a = d \cdot a',\ b = d \cdot b'$ darstellen, und sind weiterhin d und m teilerfremd, so gilt auch

$$a' \equiv b' \pmod{m}.$$

Zum **Beweis** beider Aussagen erinnern wir uns daran, dass wir $a \equiv b \pmod m$ auf drei verschiedene Arten aufschreiben können:

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

In beiden Kürzungsregeln gilt $a = d \cdot a'$, $b = d \cdot b'$, also $(a-b) = d \cdot (a'-b')$. Für die Kürzungsregel 1 schließen wir weiter

$$m = d \cdot m' \,|\, d \cdot (a'-b') \;\Rightarrow\; m' \,|\, (a'-b') \;\Rightarrow\; a' \equiv b' \;(mod\; m')$$

und für die Kürzungsregel 2 folgt aus $m \,|\, d \cdot (a'-b')$, dass $m \,|\, (a'-b')$, denn m und d waren als teilerfremd vorausgesetzt worden.

Beispiel : Aus $30 \equiv 105 \pmod{25}$ können wir also den Faktor 5 nach der 1. Kürzungsregel herauskürzen, womit sich $6 \equiv 21 \pmod 5$ ergibt. Weiter kann man den gemeinsamen Faktor 3 nach der zweiten Kürzungsregel herauskürzen. Man erhält schließlich $2 \equiv 7 \pmod 5$.

Lineare Kongruenzen

Lineare Kongruenzen sind, sehr ähnlich zu gewöhnlichen Gleichungen, Bestimmungsaufgaben, bei denen alle ganzen Zahlen zu finden sind, deren Rest eine bestimmte Bedingung erfüllt. Eine typische Aufgabe hat die Gestalt

$$71\,x \equiv 12 \pmod{93}.$$

Gesucht sind dabei alle diejenigen ganzen Zahlen x, für die $71\,x$ bei Division durch 93 den Rest 12 lässt.

Eine Lösung dieser Aufgabe ist $x = 84$. Wie man darauf kommt möge an dieser Stelle offenbleiben. Dass es wirklich eine Lösung ist, kannst Du aber einfach durch eine Probe sehen.

Da es bei einer linearen Kongruenz nicht auf die Zahl x selbst, sondern nur auf deren Rest (hier $\pmod{93}$) ankommt, ist auch jede andere Zahl mit demselben Rest eine Lösung, also etwa $x = 177, x = 270, x = 363$ usw., aber auch $x = -102, x = -9$ usw. und insgesamt jede Zahl der Form $x = 84 + k \cdot 93, k \in \mathbb{Z}$. Gibt es eine ganzzahlige Lösung, so gibt es also gleich unendlich viele. Deshalb fragen wir nicht nach den ganzzahligen Lösungen einer linearen Kongruenz, sondern nach entsprechenden Restklassen. Wir schreiben also stattdessen:

> Die Restklasse $x \equiv 84 \pmod{93}$ oder kurz $x \equiv 84 \pmod{93}$ ist eine Lösung obiger linearer Kongruenz.

Wie findet man nun alle Lösungen einer linearen Kongruenz. Die sicherste, aber auch aufwändigste Methode ist **das (vollständige !) Probieren**. Da wir wissen, dass es (ganz im Gegensatz zu den ganzen Zahlen) nur **endlich viele** Restklassen gibt, brauchen wir nur alle durchzuprobieren und die herausfiltern, für welche die Kongruenz erfüllt ist.

Dieses Verfahren ist natürlich recht aufwändig und nur dann sinnvoll, wenn es nur wenige Restklassen gibt, wenn also der Modul klein ist. Dafür kann man es nicht nur für lineare, sondern für beliebige Kongruenzen anwenden. Dafür drei Beispiele:

Aufgabe 1 Bestimme die Lösungen der linearen Kongruenz $2x \equiv 1 \pmod 3$.

Lösung: Es gibt $\pmod 3$ die Restklassen $0, 1, 2$ als mögliche Werte für x. Einsetzen zeigt, dass genau für $x \equiv 2 \pmod 3$ die obige Kongruenz erfüllt ist.

Aufgabe 2 Bestimme die Lösungen der linearen Kongruenz $3x \equiv 5 \pmod{13}$.

Lösung: Für die verschiedenen Restklassen x stellen wir die Werte in einer Tabelle zusammen:

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$3x \pmod{13}$	0	3	6	9	12	2	5	8	11	1	4	7	10

Wir sehen, dass $x \equiv 6 \pmod{13}$ die einzige Lösung ist.

Aufgabe 3 Untersuche, für welche Zahlen n die Zahl $n^3 + 2n^2 + 4$ durch 7 teilbar ist.

Lösung: Die Aufgabe kann man umformulieren: Es sind alle Restklassen $n \pmod 7$ mit $n^3 + 2n^2 + 4 \equiv 0 \pmod 7$ gesucht. Stellen wir für die 7 möglichen Reste wieder eine Tabelle auf:

n	0	1	2	3	4	5	6
$n^3 + 2n^2 + 4 \pmod 7$	4	0	6	0	2	4	5

Damit haben also genau diejenigen ganzen Zahlen n, die bei Division durch 7 einen der Reste 1 oder 3 lassen, die Eigenschaft, dass $n^3 + 2n^2 + 4$ durch 7 teilbar ist.

Manche lineare Kongruenz hat überhaupt keine Lösung. Besitzen nämlich in

$$a \cdot x \equiv b \pmod m$$

a und m einen gemeinsamen Teiler d, so muss für die Existenz einer Lösung auch $d \mid b$ gelten. Das sieht man am besten, wenn man die Kongruenz in der alternativen Form

$$a \cdot x \equiv b \pmod m \;\Leftrightarrow\; \exists\, t \in \mathbb{Z} \;:\; a \cdot x = b + m \cdot t$$

darstellt. Wegen $b = ax - mt$ ist also $gcd(a, m) \mid b$ eine *notwendige* Bedingung für die Existenz einer Lösung.

Beispiel:

$$12x \equiv 7 \;(10)$$

besitzt keine Lösung, denn $gcd(12, 10) = 2$ ist kein Teiler von 7. Und tatsächlich ist $12x$ immer eine gerade Zahl, kann also niemals auf 7 enden (genau das bedeutet ja „$\equiv 7 \;(10)$“).

Ist die notwendige Bedingung erfüllt und der Modul so groß, dass vollständiges Probieren zu aufwändig wird, so empfiehlt es sich, die lineare Kongruenz zunächst zu vereinfachen.

Beispiel:

$$12x \equiv 8 \;(10)$$

Wir reduzieren auf kleinstmögliche Reste

$$2x \equiv 8 \;(10)$$

und wenden die 1. Kürzungsregel an, um den gemeinsamen Faktor 2 herauszukürzen. Wir erhalten

$$x \equiv 4 \;(5)$$

als Lösung.

Beispiel:

$$27x \equiv 9 \ (21)$$

Wir reduzieren auf kleinstmögliche Reste

$$6x \equiv 9 \ (21)$$

und wenden die 1. Kürzungsregel an, um den gemeinsamen Faktor 3 herauszukürzen. Wir erhalten

$$2x \equiv 3 \ (7).$$

Die Lösung dieser linearen Kongruenz könnte man durch vollständiges Probieren ermitteln. Stattdessen können wir aber auch die rechte Seite gezielt durch einen gleichwertigen Rest ersetzen, der gerade ist, um dann die 2. Kürzungsregel anwenden zu können:

$$2x \equiv 3 \equiv 10 \ (7) \ \Rightarrow \ x \equiv 5 \ (7).$$

Damit haben wir die Lösung gefunden.

Attribution Section

graebe (2004-09-03):
Dieses Material wurde vor einiger Zeit als Begleitmaterial für den LSGM-Korrespondenzzirkel in der Klasse 8 erstellt und nun nach den Regeln der KoSemNet-Literatursammlung aufbereitet.