Studienmaterial
Einführung in das Rechnen mit Resten

H.-G. Gräbe, Institut für Informatik,
http://www.informatik.uni-leipzig.de/~graebe

12. April 2000

Die folgenden Ausführungen sind aus Arbeitsmaterialien zusammengestellt, die im Korrespondenzzirkel Klasse 7 und 8 der Leipziger Schülergesellschaft für Mathematik (LSGM) Verwendung finden.

Das Rechnen mit Kongruenzen. Teil 1

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 $a, b \in \mathbf{Z}$ *kongruent modulo* m sind, und schreiben

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

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:

$$a \equiv b \ (mod\ m) \ :\Leftrightarrow \ m \,|\, (a - b)$$

und können nun beweisen, dass $\equiv$ eine Äquivalenzrelation ist, indem wir die jeweilige Aussage über Kongruenzen in eine solche über Teilbarkeit umformulieren und dann unser Wissen über Teilbarkeitsaussagen anwenden:

> *Reflexivität*: Es gilt stets $a \equiv a\ (m)$, denn $m \,|\, (a - a) = 0$ (bekanntlich ist jede Zahl Teiler der Zahl 0).
>
> *Symmetrie*: Wenn $a \equiv b\ (m)$ 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 $b \equiv c\ (m)$ gilt, so gilt auch $a \equiv c\ (m)$: 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 $u \in \mathbf{Z}$ heißt *Teiler* einer Zahl $v \in \mathbf{Z}$, wenn es eine dritte Zahl $t \in \mathbf{Z}$ 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 $t \in \mathbf{Z}$ mit $a - b = m \cdot t$ gibt, oder anders

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

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

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

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

$$a \equiv b \ (m),\ c \equiv d \ (m) \ \Rightarrow \ \left\{ \begin{array}{rcll} a + c & \equiv & b + d & (m) \\ a - c & \equiv & b - d & (m) \\ a \cdot c & \equiv & b \cdot d & (m) \end{array} \right.$$

Nur bei der Division muss man vorsichtig sein !

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

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

$$a \equiv b \ (m) \ \Rightarrow \ \forall\, n \in \mathbf{N} \ a^n \equiv b^n \ (m).$$

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 $(mod\ m)$ 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 $m - 1 \equiv (-1) \ (m)$) eine wichtige Rolle.

Wir können damit Aufgaben der folgenden Art einfach lösen:

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.

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

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

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 2 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.

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

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

$a\ (mod\ 4)$	$a^2\ (mod\ 4)$
0	0
1	1
2	$4 \equiv 0$
3	$9 \equiv 1$

Aufgabe 3 Zeige, dass die Summe zweier ungerader Quadratzahlen niemals eine Quadratzahl sein kann.

Aufgabe 4 Beweise folgende Aussage: Ist die Summe zweier Quadratzahlen durch 3 teilbar, so auch jeder der beiden Summanden.

Das Rechnen mit Kongruenzen. Teil 2

Wir wollen das Arbeitsblatt 7-4 noch um zwei Rechenregeln, die das "Dividieren" von Resten betreffen, erweitern. 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

$$a \equiv b \ (mod\ m)$$

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

$$a' \equiv b' \ (mod\ m').$$

2. Kürzungsregel: Enthalten in der Kongruenz

$$a \equiv b \ (mod\ m)$$

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

$$a' \equiv b' \ (mod\ m).$$

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

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

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

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

$$71\,x \equiv 12 \ (mod\ 93).$$

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 $(mod\ 93)$) 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 $x = 84 + k \cdot 93, k \in \mathbf{Z}$. 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 $x \equiv 84 \ (mod\ 93)$ oder kurz $x \equiv 84\ (93)$ ist eine Lösung obiger linearer Kongruenz.

Wie findet man nun alle Lösungen einer linearen Kongruenz. Die sicherste, aber auch aufwendigste 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 aufwendig 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:

1. Bestimme die Lösungen der linearen Kongruenz $2x \equiv 1 \ (mod\ 3)$.

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

2. Bestimme die Lösungen der linearen Kongruenz $3x \equiv 5 \ (mod\ 13)$.

   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
$3x\ (mod\ 13)$	0	3	6	9	12	2	5	8	11	1	4	7	10

   Wir sehen, dass $x \equiv 6\ (13)$ die einzige Lösung ist.

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 $n\ (mod\ 7)$ mit $n^3 + 2n^2 + 4 \equiv 0\ (7)$ gesucht. Stellen wir für die 7 möglichen Reste wieder eine Tabelle auf:

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

$$a \cdot x \equiv b \ (mod\ m)$$

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

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

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

Beispiel : (Arbeitsmaterial, Kl. 8, S. 13)

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

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 aufwendig 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.