Rechnen mit Kongruenzen
MSG – Mathematische Schülergesellschaft
Daniel Platt

Das vorliegende Skript beschäftigt sich mit dem Thema *Rechnen mit Kongruenzen*. Das Skript entsteht entlang einer Unterrichtsreihe in der Mathematischen Schülergesellschaft (MSG) im Jahr 2013. Die vorliegende Version ist vollständig. (letzte Änderung: 04.06.2013)

Für Rückmeldungen jeder Art und insbesondere Hinweise auf Fehler bin ich sehr dankbar – am liebsten per E-Mail an plattd@math.hu-berlin.de.

Inhaltsverzeichnis

1 Vorbereitung: Potenzen

Die folgenden Fakten sollten aus dem Schulunterricht bekannt sein. Wir wiederholen sie hier der Vollständigkeit halber:

Definition 1. *Sei x eine beliebige rationale Zahl. Sei $n \geq 1$ eine beliebige natürliche Zahl. Unter der n-ten Potenz von x verstehen wir die Zahl:*

$$x^n := \underbrace{x \cdot x \cdot \dots \cdot x}_{n\text{-mal}}$$

Beispiele:

(1) $2^6 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot = 64$

(2) Für jede Zahl x gilt: $x^1 = x$.

Satz. *(Potenzrechenregeln)*

Seien k, $n \geq 2$ natürliche Zahlen. Sei x eine beliebige rationale Zahl. Dann gilt:

(i) $x^k \cdot x^n = x^{k+n}$

(ii) $\left(x^k\right)^n = x^{k \cdot n}$

Dabei ist für uns vor allem die erste Regel wichtig. Wir werden damit große Potenzen in kleinere Zerlegen. Zum Beispiel:$2^{100} = 2^{64} \cdot 2^{32} \cdot 2^4$.

2 Einstieg und typische Probleme

Das Rechnen mit Kongruenzen ist eine Methode der Zahlentheorie, also der Mathematik der ganzen Zahlen. Die Idee kommt von der Division mit Rest; das Rechnen mit Kongruenzen wird daher auch oft Rechnen mit Resten oder mit Restklassen genannt.

Rechnen mit Kongruenzen hilft bei Fragen, die mit Teilbarkeit oder Resten zu tun haben. Am Ende der folgenden drei Wochen werden wir die folgenden Fragen sehr leicht beantworten können. Ohne die nötige Theorie ist die Beantwortung aber recht kompliziert:

(1) Welchen Rest lässt die Zahl 12^{10} bei Division durch 11?

(2) Auf welche Ziffer endet die Zahl 3^{100}?

(3) Aus der österreichischen Mathematik-Olympiade 2003:

Warum ist der Ausdruck n^3+6n^2+14n für alle natürlichen Zahlen n durch 3 teilbar?

(4) Aus der (deutschen) Mathematik-Olympiade, Aufgabe `491031`:

Wie lauten die letzten drei Ziffern von 7^{2010}?

3 Rechnen mit Resten praktisch verstehen

3.1 Die Schreibweise $\equiv$

Im folgenden interessieren wir uns bei Zahlen nur für den Rest, den sie bei einer gewissen Division lassen. Zwei Zahlen, die den gleichen Rest lassen, betrachten wir zwar nicht als gleich, aber zumindest als ziemlich ähnlich.

Definition 2. *Sei $m \geq 2$ eine natürliche Zahl. Seien a, b zwei ganze Zahlen.*

a und b heißen kongruent module *m, wenn sie bei Division durch m denselben Rest lassen, also wenn zwei ganze Zahlen p_1 und p_2 existieren mit $p_1 \cdot m + a = p_2 \cdot m + b$.*

Wir schreiben dafür auch:

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

und sagen a und b sind äquivalent*.*

Beispiele:

(1) $17 \equiv 3 \pmod 7$, denn beide Zahlen lassen bei Division durch 7 den Rest 3. Mit den Bezeichnungen von oben wählen wir $p_1 = 0$ und $p_2 = 2$ und erhalten: $0 \cdot 7 + 17 = 2 \cdot 7 + 3$.

(2) $0 \equiv -5 \pmod 5$, denn $(-1) \cdot 5 + 0 = 0 \cdot 5 + (-5)$

(3) $7 \equiv -13 \pmod 2$, denn $0 \cdot 2 + 7 = 10 \cdot 2 + (-13)$

(4) $1000 \equiv -1 \pmod{13}$, denn $0 \cdot 13 + 1000 = 77 \cdot 13 + (-1)$

Wir werden nun einige Eigenschaften von äquivalenten Zahlen nennen. Diese Eigenschaften helfen uns, verschiedene Aufgaben zu lösen. Die Beweise dieser Eigenschaften liefern wir aber erst später; denn im Moment ist uns bei einigen dieser Eigenschaften noch gar nicht klar, was dort eigentlich zu beweisen ist.

Satz 1. *Für zwei ganze Zahlen a, b gilt:*

$$a \equiv b \ (mod\ m) \Leftrightarrow m \mid a - b$$

(Dabei heißt $m \mid a - b$: m teilt die Zahl $(a - b)$)

Dieser Satz hilft uns dabei, schnell zu erkennen, ob zwei Zahlen äquivalent sind. Denn so müssen wir keine geeigneten p_1 und p_2 mehr finden, sondern können einfach eine Differenz betrachten:

Beispiele:

(1) $17 \equiv 3 \pmod 7$, denn $(17-3) : 7 = 2$

(2) $1000 \equiv -1 \pmod{13}$, denn $(1000-(-1)) : 13 = 77$

3.2 Rechenregeln

Im folgenden Satz sind die wichtigsten zwei Regeln enthalten, mit denen man bereits sehr viele Aufgaben lösen kann:

Satz 2. *Seien $m \geq 2$ und a, b, a' und b' ganze Zahlen, für die gilt: $a \equiv b \pmod m$ und $a' \equiv b' \pmod m$. Dann gilt:*

(i) $a + a' \equiv b + b' \pmod m$

(ii) $a \cdot a' \equiv b \cdot b' \pmod m$

Beispiele:

(1) Es ist: $14 \equiv 1 \pmod{13}$ und $12 \equiv -1 \pmod{13}$. Damit gilt nach dem obigen Satz:

   (i) $26 \equiv 0 \pmod{13}$

   (ii) $12 \cdot 14 = 168 \equiv -1 \pmod{13}$

(2) Mit den Bezeichnungen des obigen Satzes wählen wir $m = 6$, $a = a' = 7$ und $b = b' = 1$; für diese Zahlen gilt tatsächlich $7 \equiv 1 \pmod 6$. Aus dem obigen Satz folgt dann:

   - $7 \cdot 7 = 7^2 \equiv 1 \cdot 1 = 1 \pmod 6$
   - $7 \cdot 7^2 = 7^3 \equiv 1 \cdot 1 = 1 \pmod 6$ (hier haben wir $a = 7$, $b = 1$, $a' = 7^2$, $b' = 1$ betrachtet)
   - ...
   - $7^{100} \equiv 1 \pmod 6$

(3) Es gilt $11 \equiv 1 \pmod{10}$. Mit dem Satz erhalten wir: Für jede natürliche Zahl k gilt: $11^k \equiv 1 \pmod{10}$. Oder mit anderen Worten: Jede 11er-Potenz endet mit der Ziffer 1.

Wie man schon in den Beispielen sieht, erhalten wir damit ein praktisches Verfahren, um Reste von Potenzen zu bestimmen. Wir zeigen dies am Beispiel der Frage: *Auf welche Ziffer endet* 13^{13}*?*

Gesucht ist also

$$13^{13} \equiv \ ? \pmod{10}$$

1. Wenn die Basis der betrachteten Potenz (hier: 13) größer ist als der Modul (hier: 10), so vereinfachen wir die Potenz, indem wir die Basis modulo 10 betrachten. Das heißt in unserem Fall: $13 \equiv 3 \pmod{10} \Longrightarrow$
$$13^{13} \equiv 3^{13} \pmod{10}$$

2. Wir betrachten nun also die Potenz 3^{13}. Hier bestimmen wir solange Potenzen, bis wir einen leichten Rest erhalten:
$$\begin{aligned} 3^1 = 3 &\equiv 3 \pmod{10} \\ 3^2 = 9 &\equiv 9 \pmod{10} \\ 3^3 = 27 &\equiv 7 \pmod{10} \\ 3^4 = 3^3 \cdot 3 \equiv 7 \cdot 3 &\equiv 1 \pmod{10} \end{aligned}$$
Dabei mussten wir im letzten Schritt nicht den genauen Wert 3^4 ausrechnen, sondern haben mit dem Rest 3^3 weitergerechnet.

3. Wir zerlegen jetzt die gesuchte Potenz 3^{13} in Potenzen, sodass möglichst oft die Potenz 3^4 vorkommt, weil diese ja einen sehr einfachen Rest hat.

   Wir wählen die Zerlegung:
$$3^{13} = 3^4 \cdot 3^4 \cdot 3^4 \cdot 3$$

4. Wir fassen nun alle Erkenntnisse zusammen und erhalten:
$$\begin{aligned} 13^{13} &\equiv 3^{13} && \text{(Nach 1.)} \\ &\equiv 3^4 \cdot 3^4 \cdot 3^4 \cdot 3 && \text{(Nach 3.)} \\ &\equiv 1 \cdot 1 \cdot 1 \cdot 3 && \text{(Nach 2.)} \\ &\equiv 3 \pmod{10} \end{aligned}$$
   Also endet die Zahl 13^{13} mit der Ziffer 3. Dies kann man übrigens mit einem Taschenrechner nachprüfen: Tatsächlich ist $13^{13} = 302875106592253$.

Für die Mathematikwettbewerbe Mathematik-Olympiade, Tag der Mathematik und Känguru-Wettbewerb genügt diese Wissen für viele Aufgabe. Wir betrachten trotzdem noch ein weiteres Ergebnis, das wir als Spezialfall des vorigen Satzes erhalten:
$$a \equiv b \pmod{\text{m}} \Longrightarrow a \cdot c \equiv b \cdot c \pmod{\text{m}}$$

Die Umkehrung davon gilt aber im Allgemeinen nicht (siehe Aufgaben). Sie gilt aber in einem Spezialfall trotzdem:

Satz 3. *Seien a, b, c beliebige ganze Zahlen. Sei $m \geq 2$ eine natürliche Zahl, die teilerfremd zu c ist, d.h. $ggT(c, m) = 1$. Dann gilt:*
$$a \cdot c \equiv b \cdot c \ (mod\ m) \Longrightarrow a \equiv b \ (mod\ m)$$

3.3 Anwendung für Beweise von Teilbarkeitsregeln

Viele Teilbarkeitsregeln können mit Hilfe von Kongruenzen leichter bewiesen werden, als das ohne der Fall ist. Das gilt zum einen für die uns bereits bekannten Teilbarkeitsregeln für die Teilbarkeit durch 2, 3, 5, 7, 9, 11, die man durch Modulo-Rechnungen im Dezimalsystem zeigen kann.

Man kann allerdings auch Teilbarkeitsregeln für beliebige Zahlen formulieren, diese sind aber meistens ziemlich unhandlich und sehr theoretisch. Einen Einstieg findet man zum Beispiel in http://www.uni-siegen.de/.../skripte/elzth2.pdf.

Wir werden hier eine Teilbarkeitsregel für die Teilbarkeit durch 11 beweisen:

Satz 4. *Eine beliebige Zahl $z = \overline{a_n a_{n-1} \dots a_1 a_0}$ mit $(n+1)$ Stellen ist genau dann durch 11 teilbar, wenn ihre alternierende Quersumme, also die Zahl $a_0 - a_1 + a_2 - a_3 + a_4 \pm \dots$, durch 11 teilbar ist.*

Beweis. Es ist $z = \overline{a_n a_{n-1} \dots a_1 a_0} = 10^n \cdot a_m + \dots + 10^1 \cdot a_1 + 1 \cdot a_0$.

Wir stellen fest:

$$\begin{aligned} &10 \equiv -1 \pmod{11} \\ &10^k \equiv (-1)^k \pmod{11} && \text{für alle } k \in \mathbb{N} \end{aligned}$$

Dann gilt:

$$\begin{aligned} &z \text{ ist durch 11 teilbar} \\ \Leftrightarrow\ &z \equiv 0 \pmod{11} \\ \Leftrightarrow\ &10^n \cdot a_m + \dots + 10^1 \cdot a_1 + 1 \cdot a_0 \equiv 0 \pmod{11} \\ \Leftrightarrow\ &(-1)^n \cdot a_m \dots - \cdot a_1 + 1 \cdot a_0 \equiv 0 \pmod{11} \\ \Leftrightarrow\ &\text{Die alternierende Quersumme von } z \text{ ist durch 11 teilbar} \end{aligned}$$

□

Beispiele:

(1) Wir betrachten die Zahl $z = 1085195$. Die alternierende Quersumme dieser Zahl ist $5 - 9 + 1 - 5 + 8 - 0 + 1 = 1$, also nicht durch 11 teilbar. Folglich ist auch z selbst nicht durch 11 teilbar.

Tatsächlich gilt $1085195 : 11 = 98654,\overline{09}$.

(2) Wir betrachten die Zahl $z = 6105$. Die alternierende Quersumme dieser Zahl ist $5 - 0 + 1 - 6 = 0$, also durch 11 teilbar. Folglich ist z selbst durch 11 teilbar.

Tatsächlich gilt $6105 : 11 = 555$.

Außerdem werden wir noch eine Teilbarkeitsregel für die Teilbarkeit durch 7 beweisen:

Satz 5. *Gegeben sei eine Zahl z von der Form $z = 10a + b$. Dann gilt:*

$$a - 2b \text{ ist durch 7 teilbar} \Leftrightarrow z \text{ ist durch 7 teilbar}$$

Beweis. Sei also ein $z = 10a + b$ gegeben und es gelte die Voraussetzung $a - 2b \equiv 0 \pmod 7$.

Weil $-1 \equiv -1$ gilt nach Satz 2 auch: $-a + 2b \equiv 0 \pmod 7$.

Weil $21a \equiv 0$ gilt nach dem gleichen Satz auch: $21a - a + 2b \equiv 0 \pmod 7$, also mit anderen Worten $2 \cdot (10a + b) \equiv 2 \cdot 0 \pmod 7$.

Weil 2 und 7 teilerfremd sind (d.h. $ggt(2, 7) = 1$), gilt nach Satz 3 auch:

$$10a + b \equiv 0 \pmod 7$$

das heißt aber gerade, dass $10a + b$ durch 7 teilbar ist. □

Übrigens gilt auch die Umkehrung dieser Teilbarkeitsregel. Der Beweis dazu funktioniert ziemlich ähnlich. Einzige Schwierigkeit ist es, den Kehrsatz zu formulieren und beim Beweis Voraussetzung und Behauptung nicht zu mischen.

Beispiel: Betrachten die Zahl $7168 = 10 \cdot \underbrace{716}_{=a} + \underbrace{8}_{=b}$. Es ist $716 - 2 \cdot 8 = 700$, was offensichtlich durch 7 teilbar ist. Folglich ist auch die Ausgangszahl 7168 durch 7 teilbar. (Mit dem Taschenrechner kann man nachprüfen: $7168 : 7 = 1024$).

3.4 Aufgaben

2.1) Beantworte die folgenden Fragen, die bereits in der Einleitung gestellt wurden:

(a) Welchen Rest lässt die Zahl 12^{10} bei Division durch 11?

(b) Auf welche Ziffer endet die Zahl 3^{100}?

(c) Aus der (deutschen) Mathematik-Olympiade, Aufgabe `491031`:

Wie lauten die letzten drei Ziffern von 7^{2010}?

2.2) Aus der Österreichischen Mathematikolympiade 2003: Auf welche Zahl endet 2003^{2003}?

2.3) Zeige: Ist $a \in \mathbb{Z}$ eine beliebige ungerade Zahl, so gilt $a^2 \equiv 1 \pmod 8$.

2.4) Zeige: Im Allgemeinen gilt die Aussage

$$a \cdot c \equiv b \cdot c \pmod{\mathrm{m}} \Longrightarrow a \equiv b \pmod{\mathrm{m}}$$

nicht. Finde also Zahlen a, b, $c \in \mathbb{Z}$ und $m \geq 2$, $m \in \mathbb{N}$, sodass gilt: $a \cdot c \equiv b \cdot c \pmod{\mathrm{m}}$, aber nicht gilt: $a \equiv b \pmod{\mathrm{m}}$.

2.5) Aus der ersten Mathematik-Olympiade, Aufgabe `011035`:

Mit welcher Ziffer endet die Summe $11^6 + 12^6 + 13^6 + 14^6 + 15^6 + 16^6$?

2.6) Sei p eine beliebige Primzahl, die größer als 3 ist. Zeige, dass p^2 beim Teilen durch 3 den Rest 1 lässt.

2.7) Für die Teilbarkeit durch 3 gilt die folgende Regel:

Eine Zahl ist genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist.

Einen Beweis haben wir bereits im Zirkel gegeben. Formuliere den Beweis mit Hilfe von Kongruenzen.

2.8*) Beweise die folgende Teilbarkeitsregel für die Teilbarkeit durch 7:

Gegeben sei eine Zahl $z = \overline{a_n \dots a_1 a_0 b}$. Dann: z ist genau dann durch 7 teilbar, wenn $\overline{a_n \dots a_1 a_0} - 2b$ durch 7 teilbar ist.

4 Rechnen mit Resten theoretisch verstehen

In diesem Abschnitt wollen wir die Eigenschaften von Resten beweisen, die wir bisher hemmungslos benutzt haben. Vor allem die Ergebnisse aus Satz 2 haben wir bisher benutzt, um Rechenaufgaben zu lösen. Doch auch die restlichen Eigenschaften werden wir hier beweisen.

Wir tun dies erst jetzt, da wir die modulo-Schreibweise und das $\equiv$-Symbol erst richtig verstehen wollten.

Satz 1. *Für zwei ganze Zahlen a, b gilt:*

$$a \equiv b \ (mod\ m) \Leftrightarrow m \mid a - b$$

(Dabei heißt $m \mid a - b$: m teilt die Zahl $(a - b)$)

Beweis. Beweisen die beiden Richtungen der Aussage getrennt voneinander:

"$\Longrightarrow$" Seien also a, b, m mit $a \equiv b \pmod m$ gegeben. Das heißt nach Definition: Es existieren ganze Zahlen p_1 und p_2 mit

$$\begin{aligned} & p_1 \cdot m + a = p_2 \cdot m + b \\ \Longrightarrow \quad & (p_1 - p_2) \cdot m = b - a \\ \Longrightarrow \quad & p_1 - p_2 = \frac{b-a}{m} \end{aligned}$$

Hier ist $(p_1 - p_2)$ eine ganze Zahl. Foglich steht auch auf der rechten Seite der Gleichung eine ganze Zahl. Also ist $\frac{b-a}{m}$ ganze Zahl. Das heißt aber gerade, dass m die Zahl $(b - a)$ teilt.

"$\Longleftarrow$" Seien also a, b, m mit $m \mid (b - a)$ gegeben. Folglich ist $\frac{b-a}{m}$ eine ganze Zahl. Zur Abkürzung nennen wir diese Zahl p_1. Also:

$$\begin{aligned} & p_1 = \frac{b-a}{m} \\ \Longrightarrow \quad & p_1 \cdot m = b - a \\ \Longrightarrow \quad & p_1 \cdot m + a = b \\ \Longrightarrow \quad & p_1 \cdot m + a = \underbrace{0}_{p_2} \cdot m + b \end{aligned}$$

Und nach Definition von Äquivalenz ist also $a \equiv b \pmod m$. □

Satz 2. *Seien $m \geq 2$ und a, b, a' und b' ganze Zahlen, für die gilt: $a \equiv b \ (mod\ m)$ und $a' \equiv b' \ (mod\ m)$. Dann gilt:*

(i) $a + a' \equiv b + b' \pmod{m}$

(ii) $a \cdot a' \equiv b \cdot b' \pmod{m}$

Beweis. Wir beweisen hier nur die erste Aussage, die zweite Aussage bleibt als Übungsaufgabe.

Seien also a, b, a', b', m gegeben mit $a \equiv b \pmod{m}$ und $a' \equiv b' \pmod{m}$. Nach Satz 1 ist also $m \mid b - a$ und $m \mid b' - a'$.

Die Summe von zwei durch m teilbaren Zahlen ist wieder durch m teilbar. Das heißt: $m \mid (b - a) + (b' - a')$, beziehungsweise mit anderer Klammerung:

$$m \mid (b + b') - (a + a')$$

Das bedeutet nach der Rückrichtung von Satz 1 aber gerade, dass

$$b - b' \equiv a - a' \bmod m)$$

□

Satz 3. *Seien a, b, c beliebige ganze Zahlen. Sei $m \geq 2$ eine natürliche Zahl, die teilerfremd zu c ist, d.h. $ggT(c, m) = 1$. Dann gilt:*

$$a \cdot c \equiv b \cdot c \pmod{m} \Longrightarrow a \equiv b \pmod{m}$$

Beweis.

$$\begin{aligned}
& a \cdot c \equiv b \cdot c \pmod{m} \\
\Rightarrow\ & m \mid bc - ac && \text{nach Satz 1} \\
\Rightarrow\ & m \mid (b - a)c \\
\Rightarrow\ & m \mid b - a && \text{weil } m \text{ und } c \text{ teilfremd} \\
\Rightarrow\ & a \equiv b \pmod{m}
\end{aligned}$$

□

Dabei ist die vorletzte Implikation anschaulich einigermaßen klar und wir geben uns an dieser Stelle damit zufrieden. Diese Implikation ist bekannt als *Lemma von Euklid* und man kann es wiederum beweisen, also auf noch einfachere Eigenschaften der ganzen Zahlen zurückführen. Man findet den Beweis zum Beispiel unter http://de.wikipedia.org/wiki/Lemma_von_E

4.1 Aufgaben

4.1) Beweise die zweite Aussage aus Satz 2.

5 Ausblick

5.1 Eulersche φ-Funktion

Sei n eine natürliche Zahl. Dann definieren wir:

$\varphi(n)$ = Anzahl von pos. Zahlen, die zu n teilerfremd sind, nicht größer als n sind

Dabei heißen zwei Zahlen teilerfremd, falls ihr größter gemeinsamer Teiler 1 ist. Also zum Beispiel:

- $\varphi(12) = 4$, weil nämlich die Zahlen 1, 5, 7, 11 teilerfremd zu 12 sind. Alle anderen Zahlen, die kleiner oder gleich 12 sind, aber nicht.
- $\varphi(7) = 6$, weil alle Zahlen, die kleiner als 7 sind, zu 7 teilerfremd sind.
- Allgemein gilt für jede Primzahl p:

$$\varphi(p) = p - 1$$

Mit Hilfe der φ-Funktion kann man einige interessante Aussagen formulieren und beweisen. Zwei werden hier (ohne Beweis) angegeben:

Satz 6. *(Kleiner Satz von Fermat) Für jede ganze Zahl a und jede Primzahl p gilt:*

$$a^p \equiv a \pmod{p}$$

Zwar ist dieser Satz für ganze Zahlen zwar nur von mäßigem Interesse. Allerdings kann man den Satz in verallgemeinerter Form auch anderswo anwenden.

Satz 7. *Für große Zahlen n gilt:*

$$\varphi(n) \approx n\frac{3}{\pi^2}$$

Dabei kann man ziemlich genau angeben, was in dieser Gleichung das $\approx$ bedeuten soll. Man benötigt dafür aber sehr viel Wissen über Grenzwerte und Funktionen und um diese Aussage wirklich zu verstehen, muss man vorher wahrscheinlich ein paar Jahre Mathematik studieren.

Wir überzeugen uns nur an einem Beispielen davon, dass die Abschätzung wahrscheinlich gar nicht so schlecht ist:

$$\varphi(2586486) = 738984 \approx 786197,47 = 2586486\frac{3}{\pi^2}$$

5.2 Restklassen

Wir betrachten die Teilbarkeit durch 3. Dabei fassen wir alle Zahlen, die beim Teilen durch 3 den gleichen Rest lassen, zu einer Menge zusammen. Diese Mengen nennen wir *Restklassen*. Wir erhalten also insgesamt drei Restklassen, diese nennen wir r_0, r_1, r_2:

- $r_0 = \{\dots, -6, -3, 0, 3, 6, \dots\}$
- $r_1 = \{\dots, -5, -2, 1, 4, 7, \dots\}$
- $r_2 = \{\dots, -4, -1, 2, 5, 8, \dots\}$

Also jede Zahl, die in r_0 ist, lässt beim Teilen durch 3 den Rest 0. Jede Zahl, die in r_1 ist, lässt beim Teilen durch 3 den Rest 1 und so weiter.

Und für irgendeine ganze Zahl x sei $\overline{x}$ die Restklasse, in der x liegt. Das heißt beispielsweise:

- $\overline{0} = r_0$
- $\overline{1} = r_1$
- $\overline{2} = r_2$
- $\overline{10} = r_1$
- $\overline{-3} = r_0$
- $\overline{50} = \overline{47} = \overline{-1} = r_2$
- $\dots$

Wir definieren jetzt eine Verknüpfung von zwei Restklassen. Ob diese Verknüpfung sinnvoll ist, ob sie irgendwas mit der klassischen Multiplkation zu tun hat, oder ob sie schöne Eigenschaften hat, ist uns erstmal egal. Wir definieren diese Verknüpfung $*$ einfach und schauen dann, was passiert:

Für zwei Restklassen $\overline{a}$ und $\overline{b}$ sei $\overline{a} * \overline{b} = \overline{a \cdot b}$. Dabei steht $a \cdot b$ für die ganz normale Multiplkation von zwei Zahlen.

Also beispielsweise:

- $\overline{0} * \overline{5} = \overline{0}$
- $\overline{3} * \overline{5} = \overline{15} = \overline{0}$
- $\overline{-10} * \overline{10} = \overline{-100} = \overline{2}$

Wir bemerken nun: Jede der drei Restklassen außer r_0 kann man mit einer anderen Restklasse multiplizieren, sodass r_1 herauskommt.

Das sieht erstmal ziemlich langweilig aus, ist aber in Wirklichkeit eine tiefschürfende Erkenntnis! Es gilt der folgende Satz:

Satz 8. *Sei m irgendeine Zahl und seien r_0, r_1, …, r_{m-1} die Restklassen zu m. Dann gilt:*

Wenn m eine Primzahl ist, genau dann existiert für jede Restklasse r_k außer r_0 eine andere Restklasse r_l, sodass das Produkt $r_k * r_l = r_1$ ist.

Beispiel:

- Wir betrachten $m = 4$. Dort haben wir mit r_2 ein Problem. Denn: $r_2 * r_1 = r_2$, $r_2 * r_2 = r_0$, $r_2 * r_3 = r_2$, aber nie $r_2 * r_l = r_1$!
- Wir betrachten $m = 59$. 59 ist eine Primzahl und tatsächlich stellen wir fest:
  - $r_1 * r_1 = r_1$
  - $r_2 * r_{30} = r_1$
  - $r_3 * r_{20} = r_1$
  - $r_4 * r_{15} = r_1$
  - $r_5 * r_{12} = r_1$
  - $r_6 * r_{10} = r_1$
  - $r_7 * r_{17} = r_1$
  - …