vhb - Kurs: Grundlagen der elementaren Zahlentheorie

III.4. Rechnen mit Restklassen - Beispiel: Lineare Kongruenzen

Beispielsweise soll die lineare Kongruenz

$$11X \equiv 7 \bmod 25.$$

gelöst werdem. Es gilt $11^{-1} \equiv 16 \bmod 25$ und Multiplikation unserer Kongruenz mit diesem Inversen liefert

$$X \equiv 11^{-1} \cdot 11 \equiv 11^{-1} \cdot 7 \equiv 16 \cdot 7 = 112 \equiv 12 \bmod 25.$$

Letztlich wurde diese lineare Kongruenz also ganz ähnlich gelöst, wie wir lineare Gleichungen wie z.B. $11X = 7$ lösen, nämlich durch Multiplikation mit dem Inversen des Koeffizienten 11 (welches gleich $\frac{1}{11}$ in $\mathbb{Q}$ ist).
Hierzu berechnet man für unser Eingangsbeispiel $11X \equiv 7 \bmod 25$ mit dem euklidischen Algorithmus

$$\begin{aligned} 25 &= 2 \cdot 11 + 3, \\ 11 &= 3 \cdot 3 + 2, \\ 3 &= 1 \cdot 2 + 1. \end{aligned}$$

Man liest ab, dass 11 mod 25 in der Tat eine prime Restklasse ist und findet das Inverse durch Lesen des Euklidischen Algorithmus von unten nach oben:

$$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (11 - 3 \cdot 3) = 4 \cdot 3 - 1 \cdot 11 = 4(25 - 2 \cdot 11) - 1 \cdot 11 = 4 \cdot 24 - 9 \cdot 11,$$

was modulo 25 auf eben

$$1 \equiv -9 \cdot 11 \equiv 16 \cdot 11 \bmod 25$$

führt.

Ein System linearer Kongruenzen lässt sich mit Hilfe des Chinesischen Restsatz lösen. Hier ein Beispiel:

$$\begin{cases} X \equiv 4 \bmod 6, \\ X \equiv 5 \bmod 7. \end{cases}$$

Gesucht sind die Lösungen, entweder die ganzen Zahlen, die diesen Bedingungen genügen, oder die Restklassen, welche diese Eigenschaft besitzen. Tatsächlich ist mit einer ganzen Zahl x auch jede weitere ganze Zahl $x + 42m$ mit beliebigem ganzzahligen m eine Lösung, d.h. die Lösungen bilden Restklassen modulo 42. Zur Lösung des obigen Beispiels mag man die Idee haben, durch Probieren zum Ziel zu kommen. Man sieht leicht für die Lösungsmengen der einzelnen linearen Kongruenzen:

$$\begin{aligned} X \equiv 4 \bmod 6 \quad &: \quad \ldots, 4, 10, 16, 22, 28, 34, \mathbf{40}, 46, \ldots \\ X \equiv 5 \bmod 7 \quad &: \quad \ldots, 5, 12, 19, 26, 33, \mathbf{40}, 47, \ldots. \end{aligned}$$

Man sieht, dass **40** eine Lösung beider Kongruenzen ist, also auch unseres Kongruenzsystems. Darüberhinaus sehen wir, dass es keine weitere Lösung modulo 42 gibt. Für kleine Moduln ist das eine praktikable Vorgehensweise, allerdings mag man bei großen Systemen oder wenn sehr große Moduln auftreten verzweifeln.
Beweis an unserem ersten Beispiel: Hier sind $m_1 = 6$ und $m_2 = 7$, also $m = 6 \cdot 7 = 42$ und die Lösungsformel des Beweises des chinesischen Restsatzes liefert

$$x = 4 \cdot 7^{\varphi(6)} + 5 \cdot 6^{\varphi(7)} \equiv 4 \cdot 7^2 + 5 \cdot 6^6 \equiv 40 \bmod 42.$$

Auch wenn hier mit den Potenzen der einzelnen Moduln große Zahlen stehen, so können diese doch jeweils modulo $m = 42$ reduziert werden, was diese explizite Lösungsformel auch bei Kongruenzsystemen mit recht großen Zahlen zu einem praktikablen Werkzeug macht!

Will man ein System mit paarweise teilerfremden Moduln lösen, so sieht das Verfahren etwas aufwendiger aus. Dazu betrachten wir wiederum ein Beispiel:

$$\begin{cases} X & \equiv & 2 \bmod 3, \\ X & \equiv & 3 \bmod 4, \\ X & \equiv & 5 \bmod 6. \end{cases}$$

Hier sind die Moduln offensichtlich nicht paarweise teilerfremd (denn $\mathrm{ggT}(3,6) = 3$ und $\mathrm{ggT}(4,6) = 2$). Um hier weiterzukommen, wenden wir den chinesischen Restsatz zunächst *rückwärts* an, in dem wir die letzte Kongruenz zum Modul $6 = 2 \cdot 3$ in zwei Kongruenzen modulo 2 bzw. 3 zerlegen. Tatsächlich gilt

$$X \equiv 5 \bmod 6. \qquad \Longleftrightarrow \qquad \begin{cases} X & \equiv & 1 \bmod 2, \\ X & \equiv & 2 \bmod 3. \end{cases}$$

Hier folgt die Implikation von links nach rechts einfach durch Reduktion modulo 2 bzw. 3 gemäß

$$5 \equiv 1 \bmod 2 \qquad \text{und} \qquad 5 \equiv 2 \bmod 3.$$

Die Implikation von rechts nach links hingegen ergibt sich mit dem chinesischen Restsatz (Nachrechnen!). Wir beobachten, dass eine der Kongruenzen rechts in unserem Ausgangssystem von linearen Kongruenzen bereits vorkommt. Mit dieser äquivalenten Umformung schreibt sich dieses also um zu

$$\begin{cases} X & \equiv & 1 \bmod 2, \\ X & \equiv & 2 \bmod 3, \\ X & \equiv & 3 \bmod 4. \end{cases}$$

Hier sind nun die Moduln paarweise teilerfremd und wir können das System mit dem Verfahren aus dem Beweis des chinesischen Restsatzes problemlos lösen. Nehmen wir jedoch an, in unserem Ausgangssystem stünde die Kongruenz $X \equiv 1 \bmod 3$, so folgte stattdessen die Unlösbarkeit des Systems, da keine ganze Zahl gleichzeitig in zwei inkongruenten Restklassen zu ein und demselben Modul enthalten sein kann. In jedem Fall können wir aber mit obigem Trick auch ein System linearer Kongruenzen mit nicht notwendig paarweise teilerfremden Moduln analysieren und entweder dessen Lösungsmenge explizit bestimmen oder aber die Unlösbarkeit nachweisen.

Rekapitulieren wir den Trick, den wir zur Lösung des obigen linearen Kongruenzsystems mit nicht paarweise teilerfremden Moduln herangezogen haben, so offenbart sich eine interessante Struktur der Restklassenringe. Der Einfachheit halber betrachten wir hier das obige Beispiel. Nach dem chinesischen Restsatz gilt

$$\begin{array}{ccc} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \leftrightarrow & \mathbb{Z}/2 \cdot 3\mathbb{Z} \\ (a \bmod 2, b \bmod 3) & \longleftrightarrow & c \bmod (2 \cdot 3). \end{array}$$

Hierbei steht der Pfeil '$\leftrightarrow$' für eine *eineindeutige* Korrespondenz zwischen dem Paar (a, b) links und c rechts; in obigem Beispiel war dies $(1, 2) \leftrightarrow 5$. Das dies tatsächlich eine *eineindeutige* Abbildung zwischen diesen Restklassenringen ist, beweist der chinesische Restsatz. Tatsächlich kann eine solche Korrespondenz für alle Moduln $n > 1$ mit Hilfe der Primfaktorzerlegung von n angegeben werden.