Proseminar: Angewandte diskrete Mathematik

Der Chinesische Restsatz

中国的余数定理

Proseminarvortrag von
Nadine Fuchs und Jennay Gomez Rodriguez
im November 2004 an der Universität Karlsruhe

Inhaltsverzeichnis

I. Der Chinesische Restsatz für $\mathbb{Z}/m\mathbb{Z}$

1. Grundlegendes

1.1. Defintion: Direktes Produkt von Ringen

Das direkte Produkt der (kommutativen) Ringe $A_1, \dots, A_r$ (mit Einselement) ist definiert als die Menge $A := A_1 \times \dots \times A_r$ versehen mit komponentenweiser Addition und komponentenweiser Multiplikation. Für $(x_1, \dots, x_r)$, $(y_1, \dots, y_r) \in A := A_1 \times \dots \times A_r$ sei also:
$(x_1, \dots, x_r) + (y_1, \dots, y_r) := (x_1 + y_1, \dots, x_r + y_r)$ und
$(x_1, \dots, x_r) \cdot (y_1, \dots, y_r) := (x_1 \cdot y_1, \dots, x_r \cdot y_r)$.

1.2. Folgerungen

1. $(A, +, \cdot) = (A_1 \times \dots \times A_r, +, \cdot)$ ist ein (kommutativer) Ring (mit Einselement)
2. Nullelement: (0, ..., 0)
   Einselement: (1, ..., 1)
3. Subtraktion: $-(a_1, \dots, a_r) = (-a_1, \dots, -a_r)$
   Division: $(a_1, \dots, a_r) \in A^* \Leftrightarrow a_i \in A_i^* \ \forall i = 1, \dots, r$ und $(a_1, \dots, a_r)^{-1} = (a_1^{-1}, \dots, a_r^{-1})$. Insbesondere: $A^* = A_1^* \times \dots \times A_r^*$
4. Das direkte Produkt besitzt in der Regel Nullteiler. Ein Element a eines Ringes R heißt Nullteiler, wenn es ein Element b in R gibt, wobei $b \neq 0$ ist, mit $a \cdot b = 0$.
   Sind zum Beispiel A_1, A_2 zwei Ringe mit Einselement, so gilt $(1,0) \cdot (0,1) = (0,0)$.
   Ein weiteres Beispiel für Nullteiler findet sich in den $\mathbb{R}^{2x2}-$Matrizen:
   $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

1.3. Satz

Es sei $m \in \mathbb{N}, m \geqslant 2$ und $d \in \mathbb{N}$ mit $d | m$ sei ein Teiler von m. Dann erhält man die wohldefinierte Abbildung $\pi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$
$\pi(x + m\mathbb{Z}) := x + d\mathbb{Z}$
π ist ein Ringhomomorphismus.

Beweis:

1. Beweis der Wohldefiniertheit:
   Aus $x + m\mathbb{Z} = y + m\mathbb{Z}$ folgt:
   $m | (x - y) \Rightarrow d | (x - y) \Rightarrow \pi(x + m\mathbb{Z}) = x + d\mathbb{Z} = y + d\mathbb{Z} = \pi(y + m\mathbb{Z}) \Rightarrow \pi$ ist wohldefiniert.
   Voraussetzung für die Wohldefiniertheit ist, dass d ein Teiler von m ist. Ohne diese Voraussetzung, kann es dazu kommen, dass aus $x + m\mathbb{Z} = y + m\mathbb{Z}$ nicht folgt, dass $x + d\mathbb{Z} = y + d\mathbb{Z}$ ist.
   Beispiel: $6 (\mathrm{mod}\, 7) \equiv 13 (\mathrm{mod}\, 7)$, aber $6 (\mathrm{mod}\, 2) \equiv 0 \neq 1 \equiv 13 (\mathrm{mod}\, 2)$.

2. Beweis der Homomorphismus-Eigenschaften:

$$\pi((x_1+m\mathbb{Z})+(x_2+m\mathbb{Z}))=\pi(x_1+x_2+m\mathbb{Z})=x_1+x_2+d\mathbb{Z}$$
$$=(x_1+d\mathbb{Z})+(x_2+d\mathbb{Z})=\pi(x_1+m\mathbb{Z})+\pi(x_2+m\mathbb{Z})$$
$$\forall (x_1+m\mathbb{Z}),(x_2+m\mathbb{Z})\in\mathbb{Z}/m\mathbb{Z}$$
$$\pi((x_1+m\mathbb{Z})\cdot(x_2+m\mathbb{Z}))=\pi(x_1\cdot x_2+m\mathbb{Z})=x_1\cdot x_2+d\mathbb{Z}$$
$$=(x_1+d\mathbb{Z})\cdot(x_2+d\mathbb{Z})=\pi(x_1+m\mathbb{Z})\cdot\pi(x_2+m\mathbb{Z})$$
$$\forall (x_1+m\mathbb{Z}),(x_2+m\mathbb{Z})\in\mathbb{Z}/m\mathbb{Z}$$

π ist also ein Ringhomomorphismus.

2. Der Chinesische Restsatz

2.1. Der Chinesische Restsatz

Es sei $m>1\in\mathbb{N}$ und $m=m_1\cdot\ldots\cdot m_r$ eine Zerlegung von m in paarweise teilerfremde Zahlen $m_i>1$, $m_i\in\mathbb{N}, i=1,\ldots,r$. Dann ist die natürliche Abbildung $\phi:\mathbb{Z}/m\mathbb{Z}\to(\mathbb{Z}/m_1\mathbb{Z})\times\ldots\times(\mathbb{Z}/m_r\mathbb{Z})$,

$$\phi(x+m\mathbb{Z}):=(x+m_1\mathbb{Z}),\ldots,(x+m_r\mathbb{Z})$$

ein Ringisomorphismus, also ein bijektiver Ringhomomorphismus.

Beweis:

1. Wohldefiniertheit:
   ϕ ist wohldefiniert, denn die Abbildung $\pi:\mathbb{Z}/m\mathbb{Z}\to\mathbb{Z}/d\mathbb{Z}, \pi(x+m\mathbb{Z})=x+d\mathbb{Z}$ ist nach Satz 1.3. wohldefiniert.

2. Ringhomomorphismus:
   Die Abbildung ϕ ist nach der Definition von π und der Definition des direkten Produktes ein Ringhomomorphismus.

3. Bijektivität:
   Um die Bijektivität zu zeigen, genügt es die Injektivität nachzuweisen, denn es gilt: $|\mathbb{Z}/m\mathbb{Z}|=m=m_1\cdot\ldots\cdot m_r=|\mathbb{Z}/m_1\mathbb{Z}|\cdot\ldots\cdot|\mathbb{Z}/m_r\mathbb{Z}|=|(\mathbb{Z}/m_1\mathbb{Z})\times\ldots\times(\mathbb{Z}/m_r\mathbb{Z})|$. Das heißt die Urbild- und die Bildmenge sind endliche Mengen und besitzen die gleiche Kardinalität.
   Es seien also $\bar{x},\bar{y}\in\mathbb{Z}/m\mathbb{Z}$ mit $\phi(\bar{x})=\phi(\bar{y})$. Dann folgt:
   $$0=\phi(\bar{x})-\phi(\bar{y})=\phi(\bar{x}-\bar{y})=\phi(\overline{x-y})=\phi(x-y+m\mathbb{Z})$$
   $$=((x-y+m_1\mathbb{Z}),\ldots,(x-y+m_r\mathbb{Z}))$$
   Außerdem ist $0=(0(\mathrm{mod}\, m_1),\ldots,0(\mathrm{mod}\, m_r))$.
   Daraus folgt: $m_i|(x-y)\,\forall\, i=1,\ldots,r$. Da die $m_1,\ldots,m_r$ paarweise teilerfremd sind, folgt $m|(x-y) \Rightarrow \bar{x}-\bar{y}=\overline{x-y}=\bar{0}=m\mathbb{Z}\in\mathbb{Z}/m\mathbb{Z} \Rightarrow \bar{x}=\bar{y} \Rightarrow \phi$ ist injektiv, woraus sich die Bijektivität ergibt.

2.2. Bemerkung

Der Beweis für die Surjektivität ist zwar zum Nachweis für die Bijektivität von ϕ nicht nötig. Er liefert allerdings eine Aussage über die Konstruktion der Umkehrabbildung von ϕ und wird deshalb hier trotzdem ausgeführt.

1. Dazu definiert man $e_i:=(0+m_1\mathbb{Z},...,0+m_{i-1}\mathbb{Z},1+m_i\mathbb{Z},0+m_{i+1}\mathbb{Z},...,0+m_r\mathbb{Z})$,
$$e_i\in(\mathbb{Z}/m_1\mathbb{Z})\times...\times(\mathbb{Z}/m_r\mathbb{Z})\ \ \forall i=1,...,r$$
Nun muss man zeigen, dass alle $e_i\in\text{Bild}(\phi)$ sind, d.h. $e_i\in\phi(\mathbb{Z}/m\mathbb{Z})\forall i=1,...,r$. Es gilt also Zahlen $u_i\in\mathbb{Z}$ zu finden, so dass gilt: $u_i\equiv1(\text{mod}\,m_i)$
$$u_i\equiv0(\text{mod}\,m_k)\forall k\neq i,k\in\{1,...,r\}$$
Mit $z_i:=\frac{m}{m_i}=\prod_{k\neq i} m_k,\forall i=1,...,r$ gilt: 1. $z_i\equiv0(\text{mod}\,m_k)\forall k\neq i$
2. $ggT(z_i,m_i)=1$, da alle $m_1,...,m_r$ paarweise teilerfremd sind.
Aus 2. folgt nach dem Euklidischen Algorithmus die Existenz von $y_i,k_i\in\mathbb{Z}$ (aus der linearen Darstellbarkeit des ggT) mit $y_iz_i+k_im_i=1\Leftrightarrow u_i:=y_iz_i\equiv1(\text{mod}\,m_i)$. Daraus folgt:
$u_i=y_iz_i\equiv0(\text{mod}\,m_k)\forall k\neq i$ und $u_i=y_iz_i\equiv1(\text{mod}\,m_i)$, somit also $e_i\in\text{Bild}(\phi)$.

2. Es seien $x_i\in\mathbb{Z},i=1,...,r$ beliebige ganze Zahlen, dann gilt für $x=\sum_{i=1}^{r}x_iu_i$, $x=x_1u_1+...+x_ru_r$:
$x\equiv x_iu_i\equiv x_i(\text{mod}\,m_i)$ also: $\phi(x+m\mathbb{Z})=(x+m_1\mathbb{Z},...,x+m_r\mathbb{Z})=(x_1+m_1\mathbb{Z},...,x_r+m_r\mathbb{Z})$.

2.3. Bemerkung

Eine weitere Möglichkeit den Chinesischen Restsatz zu formulieren ist die folgende:
Ein System aus simultanen Kongruenzen mit paarweise teilerfremden $m_i,i=1,...,r$ ist eindeutig lösbar.

3. Das Lösen von simultanen Kongruenzen

$x\equiv x_1(\text{mod}\,m_1)$ $\quad z_1:=\frac{m}{m_1}$ $\quad$ Mit $m_1,...,m_r\in\mathbb{N}\setminus\{1\}$ paarweise teilerfremd und $m=m_1\cdot...\cdot m_r$.

$x\equiv x_2(\text{mod}\,m_2)$ $\quad z_2:=\frac{m}{m_2}$ $\quad$ Insbesondere ist dann der $ggT(z_1,...,z_r)=1$.

$\vdots$

$x\equiv x_r(\text{mod}\,m_r)$ $\quad z_r:=\frac{m}{m_r}$

Zum Lösen simultaner Kongruenzen werden im Folgenden zwei Algorithmen aufgeführt.

3.1. Algorithmus Nr. 1 zum Lösen simultaner Kongruenzen

1. Mit Hilfe des Euklidischen Algorithmus berechnet man zuerst die lineare Darstellung des $ggT(z_1,...,z_r)$ und damit die Zahlen $y_1,...,y_r \in \mathbb{Z}$, so dass $y_1 \cdot z_1 + y_2 \cdot z_2 + ... + y_r \cdot z_r = 1$.
2. Es gilt also: $y_1 \cdot z_1 + y_2 \cdot z_2 + ... + y_r \cdot z_r = y_1 \cdot \frac{m}{m_1} + y_2 \cdot \frac{m}{m_2} + ... + y_r \cdot \frac{m}{m_r} = 1$.

   Nun definiert man $u_i := y_i \cdot z_i = y_i \cdot \frac{m}{m_i}$ und $E_i := u_i (\mathrm{mod}\, m)$, wobei $0 \leqslant E_i < m$ für alle $i = 1,...,r$. E_i ist somit der kleinste nichtnegative Rest von $u_i (\mathrm{mod}\, m)$, $i = 1,...,r$.

   Es gilt dann: 1. $E_i \equiv u_i = y_i \cdot \frac{m}{m_i} \equiv 1 (\mathrm{mod}\, m_i)$

   2. $E_i \equiv u_i = y_i \cdot \frac{m}{m_i} \equiv 0 (\mathrm{mod}\, m_k) \quad \forall k \neq i$
3. Im letzten Schritt setzt man $x \equiv x_1 \cdot u_1 + ... + x_r \cdot u_r = x_1 \cdot y_1 \cdot z_1 + ... + x_r \cdot y_r \cdot z_r \equiv x_1 \cdot E_1 + ... + x_r \cdot E_r (\mathrm{mod}\, m)$.
   Es ist also $x \equiv x_i (\mathrm{mod}\, m_i) \quad \forall i = 1,...,r$, woraus nach dem Beweis für die Surjektivität von ϕ folgt: $\phi(x + m\mathbb{Z}) = (x_1 + m_1\mathbb{Z}, x_2 + m_2\mathbb{Z}, ..., x_r + m_r\mathbb{Z})$.
   Das Ergebnis der oben stehenden Kongruenz ist die gesuchte Lösung der simultanen Kongruenzen.

3.1.1. Beispiel

Aufgabe: Löse folgende simultane Kongruenz.

$x \equiv 1 (\mathrm{mod}\, 2), \quad z_1 = \frac{30}{2} = 15$

$x \equiv 2 (\mathrm{mod}\, 3), \quad z_2 = \frac{30}{3} = 10$

$x \equiv 4 (\mathrm{mod}\, 5), \quad z_3 = \frac{30}{5} = 6$

In diesem Fall ist $m_1 = 2$, $m_2 = 3$, $m_3 = 5$ und $m = 2 \cdot 3 \cdot 5 = 30$.

1. Berechnung von y_1, y_2 und y_3:
   $ggT(15,10,6) = ggT(ggT(15,10),6) = ggT(5,6) = 1$.
   Außerdem: $15 = 1 \cdot 10 + 5, \quad 10 = 2 \cdot 5 \Rightarrow ggT(15,10) = 5 = 1 \cdot 15 - 1 \cdot 10$
   $6 = 1 \cdot 5 + 1, \quad 5 = 5 \cdot 1 \Rightarrow ggT(6,5) = 1 = 1 \cdot 6 - 1 \cdot 5$
   Daraus ergibt sich folgende lineare Darstellung des ggT(15,10,6):
   $1 = -1 \cdot 15 + 1 \cdot 10 + 1 \cdot 6$, d.h. $y_1 = -1$, $y_2 = 1$ und $y_3 = 1$.
2. Berechnung von E_1, E_2 und E_3:

$u_1 = y_1 \cdot z_1 = -1 \cdot 15 = -15$	$\equiv 1 (\mathrm{mod}\, 2)$, $\equiv 0 (\mathrm{mod}\, 3)$, $\equiv 0 (\mathrm{mod}\, 5)$,	$E_1 = 15 \equiv -15 (\mathrm{mod}\, 30)$
$u_2 = y_2 \cdot z_2 = 1 \cdot 10 = 10$	$\equiv 0 (\mathrm{mod}\, 2)$, $\equiv 1 (\mathrm{mod}\, 3)$, $\equiv 0 (\mathrm{mod}\, 5)$,	$E_2 = 10 \equiv 10 (\mathrm{mod}\, 30)$
$u_3 = y_3 \cdot z_3 = 1 \cdot 6 = 6$	$\equiv 0 (\mathrm{mod}\, 2)$, $\equiv 0 (\mathrm{mod}\, 3)$, $\equiv 1 (\mathrm{mod}\, 5)$,	$E_3 = 6 \equiv 6 (\mathrm{mod}\, 30)$

3. Setze $x \equiv 1 \cdot u_1 + 2 \cdot u_2 + 4 \cdot u_3 = 1 \cdot (-15) + 2 \cdot 10 + 4 \cdot 6 \equiv 29 (\mathrm{mod}\, 30)$
   $\equiv 1 \cdot E_1 + 2 \cdot E_2 + 4 \cdot E_3 = 1 \cdot 15 + 2 \cdot 10 + 4 \cdot 6 \equiv 59 (\mathrm{mod}\, 30)$

Die gesuchte Lösung der Kongruenz lautet also $x = 29$.

3.2. Algorithmus Nr. 2 zum Lösen simultaner Kongruenzen

$x \equiv x_1 \pmod{m_1}$ Dabei seien $m_1, \ldots, m_r \in \mathbb{N} \setminus \{1\}$ paarweise teilerfremd und $m = m_1 \cdot \ldots \cdot m_r$.
$x \equiv x_2 \pmod{m_2}$
$\vdots$
$x \equiv x_r \pmod{m_r}$

Setze $M_i := \prod_{j=1}^{i-1} m_j$ für $i = 1, \ldots, r$, also $M_1 = 1$, $M_2 = m_1$, $M_3 = m_1 \cdot m_2, \ldots$, $M_r = m_1 \cdot m_2 \cdot \ldots \cdot m_{r-1}$, $M_{r+1} = m$.
Es gilt: $ggT(M_i, m_i) = 1 \; \forall \, i = 1, \ldots, r$, das heißt es lassen sich mit Hilfe des Euklidischen Algorithmus Zahlen $v_i \in \mathbb{Z}, i = 1, \ldots, r$ finden, mit $v_i \cdot M_i \equiv 1 \pmod{m_i}$, $0 \leqslant v_i < m_i$, $i = 1, \ldots, r$.

1. Schritt:
Bilde $h_1 := x_1 \cdot v_1 \pmod{m_1}$, wobei $v_1 = 1$. Dann ist $x := h_1 \cdot M_1 \equiv x_1 \pmod{m_1}$.

2. Schritt:
Bilde $h_2 := (x_2 - h_1 \cdot M_1) \cdot v_2 \pmod{m_2}$. Dann ist:
$x := h_1 \cdot M_1 + h_2 \cdot M_2 \equiv h_1 \cdot M_1 \equiv x_1 \pmod{m_1}$, und
$x = h_1 \cdot M_1 + h_2 \cdot M_2 = h_1 \cdot M_1 + (x_2 - h_1 \cdot M_1) \cdot v_2 \cdot M_2 \equiv h_1 \cdot M_1 + x_2 - h_1 \cdot M_1 = x_2 \pmod{m_2}$.

3. Schritt:
Bilde $h_3 := (x_3 - h_1 \cdot M_1 - h_2 \cdot M_2) \cdot v_3 \pmod{m_3}$. Dann ist:
$x := h_1 \cdot M_1 + h_2 \cdot M_2 + h_3 \cdot M_3 \equiv x_1 \pmod{m_1}$, und
$x = h_1 \cdot M_1 + h_2 \cdot M_2 + h_3 \cdot M_3 \equiv h_1 \cdot M_1 + h_2 \cdot M_2 \equiv x_2 \pmod{m_2}$, und
$$x = h_1 \cdot M_1 + h_2 \cdot M_2 + h_3 \cdot M_3 = h_1 \cdot M_1 + h_2 \cdot M_2 + (x_3 - h_1 \cdot M_1 - h_2 \cdot M_2) \cdot v_3 \cdot M_3$$
$$\equiv h_1 \cdot M_1 + h_2 \cdot M_2 + x_3 - h_1 \cdot M_1 - h_2 \cdot M_2 = x_3 \pmod{m_3}.$$

j. Schritt: $(j = 1, \ldots, r)$
Bilde $h_j := (x_j - \sum_{k=1}^{j-1} h_k \cdot M_k) \cdot v_j \pmod{m_j}$. Dann gilt:
$x := \sum_{k=1}^{j} h_k \cdot M_k \equiv h_1 \cdot M_1 + \ldots + h_i \cdot M_i \equiv x_i \pmod{m_i} \; \forall \, i = 1, \ldots, j-i$, und
$$x = \sum_{k=1}^{j} h_k \cdot M_k = \sum_{k=1}^{j-1} h_k \cdot M_k + h_j \cdot M_j$$
$$= \sum_{k=1}^{j-1} h_k \cdot M_k + (x_j - \sum_{k=1}^{j-1} h_k \cdot M_k) \cdot v_j \cdot M_j$$
$$\equiv \sum_{k=1}^{j-1} h_k \cdot M_k + x_j - \sum_{k=1}^{j-1} h_k \cdot M_k = x_j \pmod{m_j}$$

Nach insgesamt r Schritten erhält man: $x = h_1 \cdot M_1 + \ldots + h_r \cdot M_r \pmod{m}$, $x \equiv x_i \pmod{m_i} \; \forall \, i = 1, \ldots, r$.

3.2.1. Beispiel

Aufgabe 1:
Ein Kartenspiel aus 56 nummerierten Karten wird in 7 Zeilen und somit 8 Spalten ausgelegt. Dann wird ein Zuschauer gebeten sich eine Karte zu merken. Anschließend wird er gefragt, in welcher Spalte seine Karte liegt. Nun werden die Karten in der Reihenfolge eigesammelt, in der sie sich zu Anfang des Spieles befunden haben und anschließend in 8 Zeilen, also 7 Spalten ausgelegt. Der Zuschauer wird wieder gefragt, in welcher Spalte sich seine Karte befindet.
Die Frage lautet nun, welche Karte sich der Zuschauer gedacht hat.

Lösung:
Nehmen wir an, die Karte lag beim ersten Mal in Spalte 4 und beim zweiten Mal in Spalte 2. Es gilt also folgende simultane Kongruenz zu lösen:

$x \equiv 4 \pmod{8} \quad \Rightarrow m = 8 \cdot 7 = 56,\ M_1 = 1,\ M_2 = 8,\ M_3 = 56$
$x \equiv 2 \pmod{7}$

Als erstes bestimmt man mit Hilfe des Euklidischen Algorithmus die Zahlen v_1 und v_2.

$v_1 \cdot M_1 \equiv 1 \pmod{m_1} \Leftrightarrow 1 = v_1 \cdot 1 + y_1 \cdot 8 \quad \Rightarrow v_1 = 1, y_1 = 0$
$v_2 \cdot M_2 \equiv 1 \pmod{m_2} \Leftrightarrow 1 = v_2 \cdot 8 + y_2 \cdot 7 \quad \Rightarrow v_2 = 1, y_2 = -1$

1. Schritt: $h_1 := x_1 \cdot v_1 \pmod{m_1} = 4 \cdot 1 \pmod{8} \equiv 4$
$x \equiv h_1 \cdot M_1 \equiv 4 \cdot 1 \equiv 4 \pmod{8}$
2. Schritt: $h_2 := (x_2 - h_1 \cdot M_1) \cdot v_2 \pmod{m_2} = (2-4) \cdot 1 \pmod{7} \equiv 5$
$x \equiv h_1 \cdot M_1 + h_2 \cdot M_2 \equiv 4 + 5 \cdot 8 \equiv 44 \pmod{56}$

Die Lösung der simultanen Kongruenz lautet also $x \equiv 44 \pmod{56}$, der Zuschauer hat also an die Karte mit der Nummer 44 gedacht.

Aufgabe 2:
Der Kleinstaat Fabelland mit 33333 Einwohnern hat eine eigene Armee. Bei Übungsmärschen geht man in 5er-Reihen – dann gehen genau 4 Offiziere an der Spitze. Bei Paraden wird in 8er-Reihen marschiert – dann ist vorne das 5-köpfige Musikkorps. Beim jährlichen Manöver gehen alle in 7er-Reihen, und es bleiben genau 3 Mann zum Ziehen der einzigen Kanone Fabellands übrig. Als einmal ein hoher Staatsbesuch kam, stellte man sich in 9er-Reihen vor dem Bahnhof auf, wobei der General und der Trompeter an der Spitze waren. In der Verfassung des Landes steht, dass höchstens 10% aller Einwohner von Fabelland in der Armee sein dürfen.
Die Frage ist nun, wieviele Soldaten Fabelland hat.

Lösung:
Auch die Lösung dieses Problems führt auf ein System aus linearen Kongruenzen, nämlich:

$x \equiv 4 \pmod{5} \quad \Rightarrow M_1 = 1,\ M_2 = 5,\ M_3 = 5 \cdot 8 = 40,\ M_4 = 5 \cdot 8 \cdot 7 = 280,\ M_5 = 5 \cdot 8 \cdot 7 \cdot 9 = 2520$
$x \equiv 5 \pmod{8}$
$x \equiv 3 \pmod{7}$
$x \equiv 2 \pmod{9}$

Als erstes muss man nun wieder die Zahlen v_1, v_2, v_3 und v_4 mit Hilfe des Euklidischen Algorithmus bestimmen.

$v_1 \cdot M_1 \equiv 1 \pmod{m_1} \Leftrightarrow 1 = v_1 \cdot 1 + y_1 \cdot 5 \quad \Rightarrow v_1 = 1, y_1 = 0$
$v_2 \cdot M_2 \equiv 1 \pmod{m_2} \Leftrightarrow 1 = v_2 \cdot 5 + y_2 \cdot 8 \quad \Rightarrow v_2 = -3, y_2 = 2$
$v_3 \cdot M_3 \equiv 1 \pmod{m_3} \Leftrightarrow 1 = v_3 \cdot 40 + y_3 \cdot 7 \quad \Rightarrow v_3 = 3, y_3 = -17$
$v_4 \cdot M_4 \equiv 1 \pmod{m_4} \Leftrightarrow 1 = v_4 \cdot 280 + y_4 \cdot 9 \quad \Rightarrow v_4 = 1, y_4 = -31$

1. Schritt: $h_1 := x_1 \cdot v_1 (\bmod m_1) = 4 \cdot 1 (\bmod 5) \equiv 4$
$x \equiv h_1 \cdot M_1 \equiv 4 \cdot 1 \equiv 4 (\bmod 5)$
2. Schritt: $h_2 := (x_2 - h_1 \cdot M_1) \cdot v_2 (\bmod m_2) = (5-4) \cdot (-3) (\bmod 8) \equiv -3 (\bmod 8) \equiv 5$
$x \equiv h_1 \cdot M_1 + h_2 \cdot M_2 \equiv 4 + 5 \cdot 5 \equiv 29 (\bmod 40)$
3. Schritt: $h_3 := (x_3 - h_1 \cdot M_1 - h_2 \cdot M_2) \cdot v_3 (\bmod m_3) = (3 - 4 - 25) \cdot 3 (\bmod 7) \equiv -78 (\bmod 7) \equiv 6$
$x \equiv h_1 \cdot M_1 + h_2 \cdot M_2 + h_3 \cdot M_3 \equiv 4 + 25 + 6 \cdot 40 \equiv 269 (\bmod 280)$
4. Schritt: $h_4 := (x_4 - h_1 \cdot M_1 - h_2 \cdot M_2 - h_3 \cdot M_3) \cdot v_4 (\bmod m_4) = (2 - 29 - 240) \cdot 1 (\bmod 9) \equiv -267 (\bmod 9) \equiv 3$
$x \equiv h_1 \cdot M_1 + h_2 \cdot M_2 + h_3 \cdot M_3 + h_4 \cdot M_4 \equiv 4 + 25 + 240 + 3 \cdot 280 \equiv 1109 (\bmod 2520)$

Als Lösung dieser Kongruenzen ergibt sich also $x \equiv 1109 (\bmod 2520)$. Nun muss als letztes noch die Bedingung berücksichtigt werden, dass es laut Verfassung nicht mehr als 3333 Soldaten in Fabelland geben darf. Da 2520 jedoch kleiner ist als 3333, ergibt sich als Lösung des Problems, dass Fabelland 1109 Soldaten besitzt.

4. Anwendung des Chinesischen Restsatzes

4.1. Addition von großen Zahlen

Es erweist sich oft als sinnvoll bei großen Zahlen eine andere Darstellungsweise der Zahlen zu wählen, nämlich in den Ringen $\mathbb{Z}/m_i\mathbb{Z}$, und dann in diesen Ringen zu rechnen. Die auf diese Weise entstehenden Teilergebnisse werden anschließend zu einem Gesamtergebnis zusammengesetzt.
Es sei $m = m_1 \cdot m_2$, $m_1, m_2 \equiv 1 (\bmod 2)$, (d.h. es handelt sich um ungerade Zahlen), $m_1, m_2 \in \mathbb{N} \setminus \{1\}$, $\mathrm{ggt}(m_1, m_2) = 1$. Daraus folgt nach dem Chinesischen Restsatz, dass zu jedem Paar $(x_1, x_2) \in \mathbb{N}_0^2$ mit $0 \leqslant x_1 < m_1$, $0 \leqslant x_2 < m_2$ genau eine Zahl $x \in \mathbb{N}_0$ existiert, wobei $0 \leqslant x < m = m_1 \cdot m_2$ und $x \equiv x_1 (\bmod m_1)$, $x \equiv x_2 (\bmod m_2)$.
Sprechweise: Die Zahl $x \in \mathbb{N}_0, 0 \leqslant x < m$ wird durch das Paar $(x_1, x_2) \in \mathbb{N}_0^2, 0 \leqslant x_1 < m_1, 0 \leqslant x_2 < m_2$ (eindeutig) repräsentiert.

Es seien $x, y \in \mathbb{Z}, 0 \leqslant x, y < m$ zwei ganze Zahlen, die durch (x_1, x_2) bzw. (y_1, y_2) repräsentiert werden, also

$$\begin{array}{lll} x \equiv x_1 (\bmod m_1) & y \equiv y_1 (\bmod m_1) & 0 \leqslant x_1, y_1 < m_1 \\ x \equiv x_2 (\bmod m_2) & y \equiv y_2 (\bmod m_2) & 0 \leqslant x_2, y_2 < m_2 \end{array}$$

Bilde

$$\begin{array}{ll} z_1 \equiv x_1 + y_1 (\bmod m_1) & 0 \leqslant z_1 < m_1 \\ z_2 \equiv x_2 + y_2 (\bmod m_2) & 0 \leqslant z_2 < m_2 \end{array}$$

Diese Additionen können parallel auf einem Rechner durchgeführt werden.

Die Zahl $z \in \mathbb{N}_0$ mit $0 \leqslant z < m$, wird also durch das Paar (z_1, z_2) eindeutig repräsentiert und es gilt:
$z \equiv z_1 \equiv x_1 + y_1 (\bmod m_1)$ Daraus folgt nach dem Chinesischen Restsatz: $z \equiv x + y (\bmod m)$.
$z \equiv z_2 \equiv x_2 + y_2 (\bmod m_2)$
Da $0 \leqslant x + y < 2m$ gilt, können zwei Fälle eintreten:
Im ersten Fall ist $z = x + y$ und somit $0 \leqslant x + y < m$, das heißt z entspricht der Summe der Zahlen x und y.
Im zweiten Fall ist $z = x + y - m$, also $m \leqslant x + y < 2m$, das heißt bei der Addition von x und y tritt ein Überlauf ein.
Aus diesem Grund ist es sinnvoll ein Verfahren zu entwickeln, welches das Problem der Überlaufkontrolle löst, das also feststellt, ob z die Summe der Zahlen x und y darstellt, oder $x + y - m$.

Die Idee dieses Verfahrens basiert auf der Lösung eines simultanen Kongruenzsystemes, dem man eine weitere Kongruenz hinzufügt:

$$\begin{array}{ll} x \equiv x_1 \pmod{m_1}, & 0 \leqslant x_1 < m_1 \\ x \equiv x_2 \pmod{m_2}, & 0 \leqslant x_2 < m_2 \end{array} \quad 0 \leqslant x < m = m_1 \cdot m_2$$

Dieses System erweitert man um eine Kongruenz $\pmod{m_0}$, $\operatorname{ggT}(m, m_0) = 1$:

$x \equiv x_3 \pmod{m_3}, \quad 0 \leqslant x_3 < m_3$

Da m_1 und m_2 ungerade gewählt wurden, ist es möglich $m_3 = 2$ zu wählen.

Es gilt also: $x \equiv x_2 \pmod{m_2} \;\Leftrightarrow\; x = x_2 + q_x \cdot m_2,\ q_x \in \mathbb{Z} \Leftrightarrow q_x \cdot m_2 = x - x_2$.

Daraus ergibt sich folgende Abschätzung (denn $0 \leqslant x_2 < m_2, 0 \leqslant x < m$):

$0 \leqslant q_x = \dfrac{x - x_2}{m_2} \leqslant \dfrac{x}{m_2} < \dfrac{m}{m_2} = m_1 \Rightarrow 0 \leqslant q_x < m_1$, das heißt q_x ist der kleinste nichtnegative Rest bei Division durch m_1, und somit die kleinste Lösung der Kongruenz $q_x \cdot m_2 = x - x_2 \equiv x_1 - x_2 \pmod{m_1}$.

Da $x = x_2 + q_x \cdot m_2$ und m_2 ungerade ist, ergibt sich: $x \equiv x_2 + q_x \equiv: x_3 \pmod 2$, $x_3 \in \{0,1\}$.

Daraus ergibt sich folgende Vorgehensweise für eine Überlaufkontrolle:

1. Man bildet $x \equiv x_3 \pmod 2$, $y \equiv y_3 \pmod 2$, $z \equiv z_3 \pmod 2$.
2. Dann gilt: i) Falls $z = x + y$, so muss auch gelten: $z_3 \equiv x_3 + y_3 \pmod 2$.
   ii) Falls $z = x + y - m$, so muss auch gelten: $z_3 \equiv x_3 + y_3 - 1 \pmod 2$.

4.1.1. Beispiel

Es seien $m_1 = 5$, $m_2 = 7$ und $m = 5 \cdot 7 = 35$.

Die erste Zahl x sei durch das Paar $(2,3)$ repräsentiert, es gilt also: $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$, woraus mit dem Chinesischen Restsatz folgt, dass $x = 17$ ist.

Die zweite Zahl y sei durch das Paar $(4,5)$ repräsentiert, es gilt also: $y \equiv 4 \pmod 5$, $y \equiv 5 \pmod 7$, woraus mit dem Chinesischen Restsatz folgt, dass $y = 19$ ist.

Außerdem gilt: $x = 3 + q_x \cdot 7 \equiv 2 \pmod 5 \;\Leftrightarrow\; q_x \cdot 7 \equiv -1 \pmod 5 \;\Leftrightarrow\; q_x \cdot 2 \equiv 4 \pmod 5 \;\Leftrightarrow\; q_x \equiv 2 \pmod 5$
also ist $q_x = 2$ und $x \equiv 3 + 2 = 5 \equiv 1 =: x_3 \pmod 2$.

Analog gilt für y: $y = 5 + q_y \cdot 7 \equiv 4 \pmod 5 \;\Leftrightarrow\; q_y \cdot 7 \equiv -1 \pmod 5 \;\Leftrightarrow\; q_y \cdot 2 \equiv 4 \pmod 5 \;\Leftrightarrow\; q_y \equiv 2 \pmod 5$
also ist $q_y = 2$ und $y \equiv 5 + 2 = 7 \equiv 1 =: y_3 \pmod 2$.

Bei der Addition von x und y ergibt sich nun:

$z \equiv x_1 + y_1 = 2 + 4 = 6 \equiv 1 \pmod 5 =: z_1$

$z \equiv x_2 + y_2 = 3 + 5 = 8 \equiv 1 \pmod 7 =: z_2$

Mit dem Chinesischen Restsatz folgt hieraus, dass durch das Paar $(1,1)$ die Zahl $z = 1$ repräsentiert wird.

Außerdem gilt: $z = 1 + q_z \cdot 7 \equiv 1 \pmod 5 \;\Leftrightarrow\; q_z \cdot 7 \equiv 0 \pmod 5 \;\Leftrightarrow\; q_z \equiv 0 \pmod 5$
also ist $q_z = 0$ und $z \equiv 1 \pmod 2$.

Weiter gilt: $x + y \equiv x_3 + y_3 = 1 + 1 \equiv 0 \pmod 2$, aber $z \equiv 1 \pmod 2$. Bei der Addition von x und y ist also ein Überlauf eingetreten. Das heißt die durch das Paar (z_1, z_2) repräsentierte Zahl $z \in \mathbb{N}_0$, $0 \leqslant z < 35$, ist gleich $x + y - 35 = 17 + 19 - 35 = 1$ und nicht gleich der Summe von x und y.

5. Das Lösen von nicht teilerfremden Kongruenzen

5.1. Satz

Es seien $x_1, x_2 \in \mathbb{Z}$, $m_1, m_2 \in \mathbb{N}$, und es gelte: $ggT(m_1, m_2) = d > 1$.
Die simultane Kongruenz $x \equiv x_1 (\text{mod } m_1)$, $x \equiv x_2 (\text{mod } m_2)$ ist genau dann lösbar, wenn d ein Teiler von $(x_1 - x_2)$ ist.

Beweis:

„ $\Rightarrow$ "
Die simultane Kongruenz $x \equiv x_1 (\text{mod } m_1)$, $x \equiv x_2 (\text{mod } m_2)$ sei lösbar, d.h. es gibt ein $x \in \mathbb{Z}$ mit $x = x_1 + k_1 \cdot m_1 = x_2 + k_2 \cdot m_2$ mit $k_1, k_2 \in \mathbb{Z}$.
Es folgt $x_1 - x_2 = k_2 \cdot m_2 - k_1 \cdot m_1$.
Wegen $d = ggT(m_1, m_2) | m_1$ und $d | m_2$ folgt $d | (k_2 \cdot m_2 - k_1 \cdot m_1) = x_1 - x_2$.

„ $\Leftarrow$ "
Es gelte $d = ggT(m_1, m_2) | (x_1 - x_2)$, also $x_1 - x_2 = \alpha \cdot d$ mit $\alpha \in \mathbb{Z}$. Dann existieren $k_1, k_2 \in \mathbb{Z}$ mit $d = ggT(m_1, m_2) = k_1 \cdot m_1 + k_2 \cdot m_2$.
Durch Multiplikation mit α ergibt sich $\alpha \cdot k_1 \cdot m_1 + \alpha \cdot k_2 \cdot m_2 = \alpha \cdot d = x_1 - x_2$, also $x := x_1 - \alpha \cdot k_1 \cdot m_1 = x_2 + \alpha \cdot k_2 \cdot m_2$, und es gilt: $x \equiv x_1 (\text{mod } m_1)$, $x \equiv x_2 (\text{mod } m_2)$.

Der Beweis wird hier nur für zwei Kongruenzen gezeigt. Für mehrere Kongruenzen ist der Beweis allerdings ähnlich, denn hier muss man zeigen, dass $\forall i \neq j$ gilt: $ggT(m_i, m_j) | a_i - a_j$.

5.2. Beispiel: Die Eieraufgabe von Brahmagupta

Eine alte Frau geht über den Marktplatz. Ein Pferd tritt auf ihre Tasche und zerbricht die gekauften Eier. Der Besitzer des Pferdes möchte den Schaden ersetzen und fragt die alte Frau, wie viele Eier in ihrer Tasche waren. Sie weiß die exakte Zahl nicht mehr, aber sie erinnert sich, dass genau ein Ei übrig bleibt, wenn sie beim Auspacken die Eier immer zu zweit aus der Tasche nimmt. Das Gleiche geschieht, wenn sie die Eier immer zu dritt, zu viert, zu fünft und zu sechst aus der Tasche nimmt. Nur wenn sie die Eier zu siebt aus der Tasche nimmt, bliebt kein Ei übrig. Was ist die kleinste Zahl an Eiern, welche die alte Frau in ihrer Tasche haben kann?

Lösung:

Zu lösen ist das folgende lineare Kongruenzensystem:
$x \equiv 1 (\text{mod } 2)$, $x \equiv 1 (\text{mod } 3)$, $x \equiv 1 (\text{mod } 4)$,
$x \equiv 1 (\text{mod } 5)$, $x \equiv 1 (\text{mod } 6)$, $x \equiv 0 (\text{mod } 7)$.

Die Vorausetzungen für die Lösbarkeit dieses Systems sind für die nicht teilerfremden Kongruenzen erfüllt:
$ggT(2,6) = 2$ und $2 | 1 - 1$
$ggT(2,4) = 2$ und $2 | 1 - 1$
$ggT(3,6) = 3$ und $3 | 1 - 1$
$ggT(4,6) = 2$ und $2 | 1 - 1$

Erste Kongruenz: $x \equiv 1 \pmod 2 \Leftrightarrow x = 1 + k_1 \cdot 2$ mit $k_1 \in \mathbb{Z}$.

Zweite Kongruenz: $x = 1 + k_1 \cdot 2 \equiv 1 \pmod 3 \Leftrightarrow k_1 \cdot 2 \equiv 0 \pmod 3$

$$\Leftrightarrow k_1 \equiv 0 \pmod 3 \Leftrightarrow k_1 = k_2 \cdot 3 \text{ mit } k_2 \in \mathbb{Z}$$

also

$$x = 1 + k_2 \cdot 6 \text{ mit } k_2 \in \mathbb{Z}.$$

Dritte Kongruenz: $x = 1 + k_2 \cdot 6 \equiv 1 \pmod 4 \Leftrightarrow k_2 \cdot 6 \equiv 0 \pmod 4$

$$\Leftrightarrow k_1 \equiv 0 \pmod 2 \Leftrightarrow k_2 = k_3 \cdot 2 \text{ mit } k_3 \in \mathbb{Z}$$

also

$$x = 1 + k_3 \cdot 12 \text{ mit } k_3 \in \mathbb{Z}.$$

Vierte Kongruenz: $x = 1 + k_3 \cdot 12 \equiv 1 \pmod 5 \Leftrightarrow k_3 \cdot 12 \equiv 0 \pmod 5$

$$\Leftrightarrow k_3 \equiv 0 \pmod 5 \Leftrightarrow k_3 = k_4 \cdot 5 \text{ mit } k_4 \in \mathbb{Z}$$

also

$$x = 1 + k_4 \cdot 60 \text{ mit } k_4 \in \mathbb{Z}.$$

Fünfte Kongruenz: $x = 1 + k_4 \cdot 60 \equiv 1 \pmod 6$.

Diese Konkruenz ist für alle $k_4 \in \mathbb{Z}$ erfüllt, stellt also keine neue Forderung an die gesuchte Anzahl dar.

Sechste Kongruenz: $x = 1 + k_4 \cdot 60 \equiv 0 \pmod 7 \Leftrightarrow k_4 \cdot 60 \equiv -1 \equiv 6 \pmod 7$

$$\Leftrightarrow k_4 \cdot 10 \equiv 1 \pmod 7 \Leftrightarrow k_4 \cdot 3 \equiv 1 \pmod 7 \ | \cdot 5$$

$$\Leftrightarrow k_4 \cdot 15 \equiv k_4 \equiv 5 \pmod 7 \Leftrightarrow k_4 = 5 + k_5 \cdot 7 \text{ mit } k_5 \in \mathbb{Z}$$

also

$$x = 1 + (5 + k_5 \cdot 7) \cdot 60 = 301 + k_5 \cdot 420 \text{ mit } k_5 \in \mathbb{Z}.$$

Ergebnis:
Die alte Frau hat mindestens 301 Eier in ihrer Tasche.

6. Brahmagupta

6.1. Biographisches

Brahmagupta war ein bedeutender indischer Mathematiker und Astronom.
Er ist um 598 im Nordwesten Indiens geboren. Die meiste Zeit seines Lebens verbrachte er in Bihillhamala (heute Bhinmal in Rajasthan). Er wirkte und lehrte an der Ujjain-Schule, die damals das mathematische Zentrum Indiens war. Brahmagupta und weitere indische Mathematiker trugen dazu bei, dass die mathematische Astronomie die große Stärke der Schule wurde.
Brahmagupta wurde auch zum Leiter des Observatoriums in Ujjain ernannt.
628 schrieb er sein bekanntes Werk Brahmasphutasiddhanten.
Dieses Werk besteht aus 25 Kapiteln, wobei der größte Teil sich der Astronomie widmet. Allein zwei Kapitel sind mathematischer Natur, das 12. Kapitel Ganita (Arithmetik) und das 18. Kapitel Kuttaka (Algebra).
Brahmagupta definiert in diesem Buch zum ersten Mal die Null als Zahl und die negativen Zahlen. Für die damalige Zeit war dies etwas völlig Neues und es forderte auch ein stärkeres abstraktes Denken.
Weiterer mathematischer Inhalt wären z.B. die Methoden zum Lösen quadratischer Gleichungen, die er gefunden hat, sowie die Methoden der Multiplikation und der Algorithmus zum Berechnen von Quadratwurzeln.
665 verfasste er sein zweites bekanntes Werk Khandahadyaka.
Dieses Buch ist in acht Kapitel unterteilt und ist wieder hauptsächlich astronomischen Inhalts. Der mathematische Schwerpunkt dieses Buches ist die Interpolationsformel, die er zum Berechnen von Sinuswerten benutzte.
Er starb 668 im Alter von 70 Jahren.

II. Kongruenzrelationen in K[X]

1. Grundlegendes

1.1. Definition

K sei ein Körper und $R := K[X]$ der Polynomring in der Unbestimmten X über dem Körper K. Sei $m \in R \setminus K$ ein Polynom mit $\deg(m) \geqslant 1$. Dann ist die Kongruenzenrelation modulo m im Ring $R := K[X]$ definiert durch $f \equiv g (\text{mod } m),\ f, g \in R \Leftrightarrow m | (f-g) \Leftrightarrow f-g \in (m) = mK[X]$.

1.2. Bemerkungen

1. Durch $f \equiv g (\text{mod } m), f, g \in R \Leftrightarrow m | (f-g)$ wird eine Äquivalenzrelation auf R definiert.

2. Aus $f_1 \equiv g_1 (\text{mod } m)$ und $f_2 \equiv g_2 (\text{mod } m)$, $f_1, f_2, g_1, g_2 \in R$ folgt $f_1 \pm f_2 \equiv g_1 \pm g_2 (\text{mod } m)$ und $f_1 \cdot f_2 \equiv g_1 \cdot g_2 (\text{mod } m)$.

3. $\bar{f} := \{f + qm \mid q \in R\} = f + (m)$ bezeichnet die Äquivalenzklasse (Kongruenzklasse mod m) des Polynoms $f \in R$.
   Die Menge der Kongruenzklassen mod m werde mit R/(m)=K[X]/(m) bezeichnet.

   Addition und Multiplikation auf K[X]/(m):
   $\bar{f} + \bar{g} := \overline{f+g}$ und $\bar{f} \cdot \bar{g} := \overline{f \cdot g},\ \bar{f}, \bar{g} \in K[X]/(m)$.

   (K[X]/(m),+, $\cdot$) ist ein kommutativer Ring mit Eins.
   Dieser Ring ist in der Regel nicht nullteilerfrei.

4. Es sei $p \in K[X]$ ein irreduzibles Polynom (Primelement in K[X]). Wenn das gilt, ist (K[X]/(p),+, $\cdot$) ein Körper.

5. Der Ring (K[x]/(m),+, $\cdot$) ist genau dann ein Körper, wenn m ein irreduzibles Polynom in K[X] ist.

Beweis:

zu 1. Z.z. Reflexivität, Symmetrie und Transitivität der Relation:

$$f \equiv g (\text{mod } m) :\Leftrightarrow m | (f-g) \Leftrightarrow f-g \in (m) = m \cdot K[X].$$

i) Reflexivität:
$\forall f \in K[X] : f \equiv f (\text{mod}\, m)$ wegen $m | (f-f) = 0$.

ii) Symmetrie:
$\forall f, g \in K[X] : f \equiv g (\text{mod } m) \Leftrightarrow m | (f-g) \Leftrightarrow m | (g-f) \Leftrightarrow g \equiv f (\text{mod } m)$.

iii) Transitivität
$\forall f, g, h \in K[X] : f \equiv g (\text{mod } m) \text{und}\, g \equiv h (\text{mod } m)$
$\Rightarrow m | (f-g) \text{und}\, m | (g-h) \Rightarrow m | (f-g) + (g-h) = (f-h)$
$\Rightarrow f \equiv h (\text{mod } m)$.

zu 2. Es gilt:

i) $f_1 \equiv g_1 (\text{mod } m)$ und $f_2 \equiv g_2 (\text{mod } m) \Leftrightarrow m|(f_1 - g_1)$ und $m|(f_2 - g_2)$
$\Rightarrow m|(f_1 \pm f_2) - (g_1 \pm g_2) \Rightarrow f_1 \pm f_2 \equiv g_1 \pm g_2 (\text{mod } m)$

ii) $f_1 \equiv g_1 (\text{mod } m)$ und $f_2 \equiv g_2 (\text{mod } m) \Leftrightarrow m|(f_1 - g_1)$ und $m|(f_2 - g_2)$
$\Rightarrow m|f_1 \cdot (f_2 - g_2) + g_2 \cdot (f_1 - g_1) = f_1 \cdot f_2 - g_1 \cdot g_2$
$\Rightarrow f_1 \cdot f_2 \equiv g_1 \cdot g_2 (\text{mod } m)$

zu 3. Die Addition sowie die Multiplikation auf K[X]/m sind nach 2. wohldefiniert:
$\bar{f} + \bar{g} := \overline{f+g}$ und $\bar{f} \cdot \bar{g} := \overline{f \cdot g}$ für $f, g \in K[X]$
(K[X]/(m),+, ·) ist ein kommutativer Ring mit Einselement. Genauer ergibt sich:

i) (K[X]/(m),+) ist eine abelsche Gruppe mit dem Nullelement $\bar{0} = 0 + (m) = (m)$
und der Subtraktion $-\bar{f} = \overline{-f}$.

ii) (K[X]/(m), ·) ist eine abelsche Halbgruppe mit dem Einselement:
$\bar{1} = 1 + (m)$.

iii) In (K[X]/(m),+, ·) gelten die Distributivgesetze.
<u>Beachte</u>: Die üblichen Rechengesetze gelten in (K[X]/(m),+, ·), da sie in K[X] gelten.

iv) Der Ring (K[X]/(m),+, ·) ist normalerweise <u>nicht nullteilerfrei</u>, denn ist das Polynom
$m \in K[x]$ reduzibel in K[X], gilt also
$m = m_1 \cdot m_2$ mit $m_1, m_2 \in K[X]$, $\deg(m_1) \geqslant 1$, $\deg(m_2) \geqslant 1$,
so gilt in (K[X]/(m),+, ·)
$\overline{m_1} \neq \bar{0}$ und $\overline{m_2} \neq \bar{0}$, aber $\overline{m_1} \cdot \overline{m_2} = \overline{m_1 \cdot m_2} = \bar{m} = \bar{0}$.

zu 4. <u>Behauptung</u>: $p \in K[x]$ irreduzibel ⇒ (K[x]/(p),+, ·) ist ein Körper.

<u>Beweis:</u> Es sei $\bar{f} = f + (p) \in K[x]/(p)$, $\bar{f} \neq \bar{0} = (p)$.
Z.z.: $\bar{f}$ ist in K[X]/(p) invertierbar, d.h. dass es zu $\bar{f}$ ein Polynom $g \in K[X]$ gibt,
mit $\bar{f} \cdot \bar{g} = \overline{f \cdot g} = \bar{1}$.

Es sei $f \in \bar{f}$. Wegen $\bar{f} \neq \bar{0}$ folgt $p \nmid f$.
Da das Polynom $p \in K[X]$ ist, folgt ggT(f,p)=1.
Also gibt es Polynome $g, h \in K[X]$ mit $g \cdot f + h \cdot p = 1$,
also $g \cdot f \equiv 1 (\text{mod } m) \Leftrightarrow \bar{g} \cdot \bar{f} = \overline{g \cdot f} = \bar{1}$.

zu 5. <u>Behauptung:</u> Ist (K[X]/(m),+, ·) ein Körper, so ist das Polynom $m \in K[X]$ irreduzibel in K[X].

<u>Beweis:</u> Wenn das Polynom m in K[X] reduzibel ist, dann gibt es Polynome
$m_1, m_2 \in K[X]$ mit $\deg(m_2) \geqslant 1$ und $m(X) = m_1(X) \cdot m_2(X)$.

Wegen $\deg(m) = \deg(m_1) + \deg(m_2)$, gilt $\deg(m_1) < \deg(m)$ und $\deg(m_2) < \deg(m)$,
also $m \nmid m_1$ und $m \nmid m_2$, also $\overline{m_1} \neq \bar{0}$ und $\overline{m_2} \neq \bar{0}$.
Man beachte $\bar{m} = \overline{m_1 \cdot m_2} = \overline{m_1} \cdot \overline{m_2} = \bar{0}$
⇒ der Ring K[X]/(m) ist nicht nullteilerfrei ⇒ K[X]/(m) ist also kein Körper.

1.3. Beispiel: Der Körper mit 4 Elementen

Sei speziell $K=F_2=\{0,1\}$ und $m(X):=X^2+X+1$.
Das Polynom m(X) ist irreduzibel in $F_2[X]$ $\Rightarrow$ der Restklassenring $(F_2[X]/(m),+,\cdot)$ ist ein Körper. .
Nach Division mit Rest ergibt sich:
$f(X)=q(X)\cdot(X^2+X+1)+r(X),\ \ f,q,r\in F_2[X]$ mit $r(X)=0$ oder $0\leqslant\deg(r(X))\leqslant 1$.
Somit folgt für r(X): r(X)=0, 1, X, X+1,
und es folgt
$F_4:=F_2[X]/(X^2+X+1)=\{\overline{0},\ \overline{1},\ \overline{X},\ \overline{X+1}\}$. Die folgenden Divisionen in $F_2[X]$ führen zu der untenstehenden Multiplikationstabelle des Körpers F_4 .

- $X^2=1\cdot(X^2+X+1)+(X+1)\Rightarrow\overline{X}^{\,2}=\overline{X^2}=\overline{(X+1)}$
- $X\cdot(X+1)=(X+1)\cdot X=X^2+X=1\cdot(X^2+X+1)+1$
  $\Rightarrow\overline{X}\cdot\overline{X+1}=\overline{X+1}\cdot\overline{X}=\overline{X\cdot(X+1)}=\overline{1}$
- $(X+1)^2=x^2+1=1\cdot(X^2+X+1)+X\Rightarrow\overline{X+1}^{\,2}=\overline{(X+1)^2}=\overline{X}$

Multiplikationstabelle im Körper F_4

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{X}$	$\overline{0}$	$\overline{X}$	$\overline{X+1}$	$\overline{1}$
$\overline{X+1}$	$\overline{0}$	$\overline{X+1}$	$\overline{1}$	$\overline{X}$

2. Der Chinesische Restsatz für Polynome

2.1. Theorem

Es sei K ein Körper, K[X] der Polynomring in der Unbestimmten X über dem Körper K und
$m\in K[X],\deg(m)\geqslant 1$. Außerdem gelte $m=m_1\cdot m_2\cdot\ldots\cdot m_r,\ m_i\in K[X]$,
$\deg(m_i)\geqslant 1\quad\forall i=1,\ldots,r,\quad ggT(m_i,m_j)=1\quad\forall i,j=1,\ldots,r$ mit $i\neq j$.
Dann ist die Abbildung

$$\pi: K[X]/(m)\to K[X]/(m_1)\times\ldots\times K[X]/(m_r),$$
$$\overline{f}=f+(m)\to\pi(\overline{f}):=(f+(m_1),\ldots,f+(m_r))$$

ein Ring-Isomorphismus, d.h. ein bijektiver Ring-Homomorphismus.

Beweis:

1. Klar: π ist ein Ringhomomorphismus, d.h. es gilt
   $\pi(\overline{f}+\overline{g})=\pi(\overline{f})+\pi(\overline{g})$ und $\pi(\overline{f}\cdot\overline{g})=\pi(\overline{f})\cdot\pi(\overline{g})$

2. π ist injektiv, denn es seien $\overline{f}=f+(m),\ \ \overline{g}=g+(m)\in K[X]/(m)$, weiter gelte $\pi(\overline{f})=\pi(\overline{g})$
   also $m_i|(f-g)\quad\forall i=1,\ldots,r$.
   Der $ggT(m_i,m_j)=1\quad\forall i,j\in\{1,\ldots,r\}$ mit $i\neq j$, denn alle m_i sind paarweise teilerfremd
   $\Rightarrow m=m_1\cdot m_2\cdot\ldots\cdot m_r|(f-g)$
   also $\overline{f}=\overline{g}$
   $\Rightarrow\pi$ ist injektiv.

3. Z.z. π ist surjektiv.

Definiere $z_i := \frac{m}{m_i}$, $i=1,\dots,r$.

Der $ggT(z_1,\dots,z_r)=1$, es gibt also Polynome $y_1,\dots,y_r \in K[X]$ mit

$$y_1 \cdot z_1 + \dots + y_r \cdot z_r = 1 \qquad \text{(lineare Darstellung des ggT).}$$

Es sei $(f_1+(m_1),\dots,f_r+(m_r)) \in K[X]/(m_1) \times \dots \times K[X]/(m_r)$.

Setze $f \equiv f_1 \cdot y_1 \cdot z_1 + \dots + f_r \cdot y_r \cdot z_r \pmod{m}$.

Es gilt $y_i \cdot z_i \equiv 1 \pmod{m_i}$ und $y_i \cdot z_i \equiv 0 \pmod{m_j}$ $\forall j \neq i$, $i,j \in \{1,\dots,r\}$,

$\Rightarrow$ $\pi(\bar{f}) = (f_1+(m_1),\dots,f_r+(m_r))$.

(vgl. mit dem Beweis für den Chinesischen Restsatz in $\mathbb{Z}$)

2.2. Anwendung: Polynominterpolation

2.2.1. Interpolation in der Praxis

Ein Gebiet, in dem Interpolation gebraucht wird, ist z.B. die Geowissenschaft.
Eines der größten Probleme in der Geowissenschaft ist es, kontinuierliche topografische Informationen einer bestimmten Region in angemessene Daten zu überführen.
Die Interpolation wird hier nun gebraucht, um durch wenige Daten eine kontinuierliche Funktion aufzustellen und die topografische Oberfläche der gewünschten Region wiederzugeben. Speziell wird die Interpolation verwendet, um Höhenunterschiede darzustellen.

Ein weiteres Anwendungsgebiet ist die Auswertung eines Experimentes. Durch ein Experiment erhält man keine kontinuierlichen Werteaufzeichnungen, da nur einzelne Messungswerte zu bestimmten Zeitpunkten enstehen. Durch die Interpolation können Werte für Zeitpunkte bestimmt werden, an denen keine Messung stattfand. Jetzt erhält man auch eine kontinuierliche Funktion im Koordinatensytem und keine einzelnen Punkte mehr.
Ein konkretes Beispiel kommt aus der Elektrotechnik, in dem es um die Entladung eines Kondensators geht.
Die Messung beginnt zum Zeitpunkt t=0 und wird in immer gleichbleibenden Abständen wiederholt. Die Zeitintervalle entsprechen den Stützstellen und die Spannungs- bzw die Stromwerte den Funktionswerten. Durch die Interpolation erhält man, im Gegensatz zu punktuellen Messwerten, eine Funktion, die sich der Exponentialfunktion annähert.

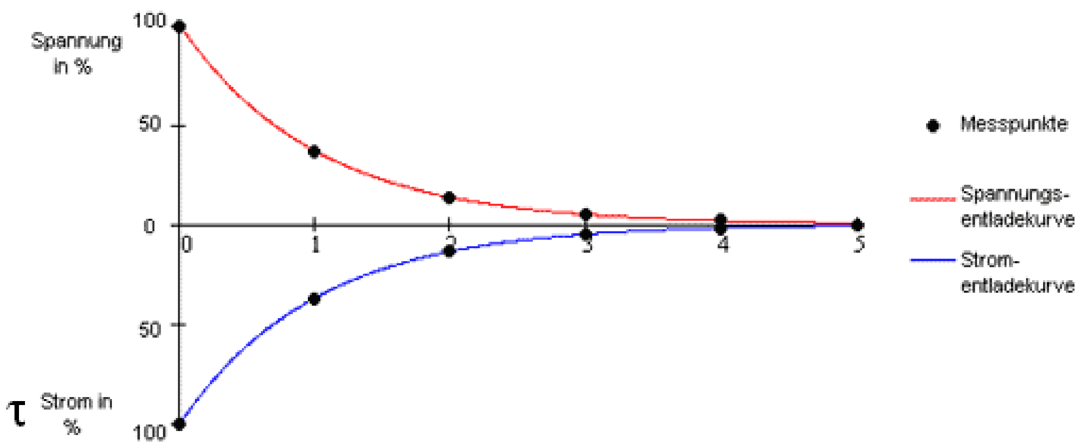

Abb.: Entladung eines Kondensators, aus Messpunkten resultierende Funktionen

2.2.2. Definition

Es seien $x_1, x_2, \ldots, x_n, x_{n+1} \in \mathbb{R}$, $n \in \mathbb{N}$, paarweise verschiedene reelle Zahlen und $(b_1, b_2, \ldots, b_n, b_{n+1}) \in \mathbb{R}^{n+1}$.

1. Es gibt genau ein Polynom $f(X) \in \mathbb{R}[X]$ mit $\deg(f) \leqslant n$ und $f(x_i) = b_i \quad \forall i = 1, \ldots, n+1$
2. Die Aufgabe, ein derartiges **Interpolationspolynom** f zu finden, ist äquivalent mit der Aufgabe, das folgende simultane Kongruenzsystem zu lösen:

$$f \equiv b_1 (\mathrm{mod}\ (X - x_1)),\ \ f \equiv b_2 (\mathrm{mod}\ (X - x_2)), \ldots,$$
$$f \equiv b_n (\mathrm{mod}\ (X - x_n)),\ \ f \equiv b_{n+1} (\mathrm{mod}\ (X - x_{n+1})).$$

Existenz: Definiere

$$f_j(X) := \prod_{k=1, k \neq j}^{n+1} \frac{X - x_k}{x_j - x_k}, \qquad j = 1, \ldots, n+1.$$

Es gilt

$$f_j(x_j) = 1,\ f_j(x_k) = 0 \quad \forall k = 1, \ldots, n+1 \text{ mit } k \neq j,\ j = 1, \ldots, n+1$$
$$\deg(f_j(X)) = n \quad \forall j = 1, \ldots, n+1.$$

Definiere

$$f(X) := \sum_{j=1}^{n+1} b_j \cdot f_j(X)\ .\ (\textbf{Interpolationsformel von Lagrange})$$

Es gilt

$$f(X) \in \mathbb{R}[X],\ \deg(f(X)) \leqslant n \text{ und } f(x_j) = b_j \quad \forall j = 1, \ldots, n+1.$$

Eindeutigkeit:
Seien $f(X), g(X) \in \mathbb{R}[X]$, und sei $f(x_j) = b_j = g(x_j) \ \ \forall \ \ j = 1, \ldots, n+1$ und $\deg(f) \leqslant n$, $\deg(g) \leqslant n$.
Somit hat das Polynom $f(X) - g(X)$ die $(n+1)$ Nullstellen $x_1, x_2, \ldots, x_n, x_{n+1}$, und es gilt $\deg(f(X) - g(X)) \leqslant n$
$\Rightarrow f(X) = g(X)$.
Die Kongruenz $f(X) \equiv b_j (\mathrm{mod}\ (X - x_j))$, $f(X) \in \mathbb{R}[X]$, ist gleichwertig mit $f(X) = b_j + q_j (X - x_j)$ mit $q_j \in \mathbb{R}[X]$,
also mit $f(x_j) = b_j$.
Die Aufgabe: Lösen des linearen Kongruenzsystems
$f_j(X) \equiv b_j (\mathrm{mod}\ (X - x_j))$, $j = 1, \ldots, n+1$,
bedeutet also, ein Polynom zu finden, dessen Graph durch die Punkte (x_j, b_j), $j = 1, \ldots, n+1$ verläuft.

2.2.3. Beispiel

Sei $K=\mathbb{R}$. Im Polynomring $\mathbb{R}[X]$ sei das folgende Kongruenzsystem zu lösen:
$f\equiv 1(\mathrm{mod}\ (X-1))$, $f\equiv 2(\mathrm{mod}\ (X-2))$, $f\equiv -1(\mathrm{mod}(X-3))$
Die Aufgabe besteht nun darin, ein Polynom $f\in\mathbb{R}[X]$ zu finden, für das gelten muss
$f(1)=1$, $f(2)=2$, $f(3)=-1$ und $\deg(f)\leqslant 2$.

Um diese Aufgabe zu lösen, kann der selbe Algorithmus verwendet werden, welcher schon benutzt wurde, um die simultanen Kongruenzen in $\mathbb{Z}$ zu lösen.

Um ein Interpolationspolynom f_0 mit $\deg(f_0)\leqslant 2$ zu erhalten, muss das erhaltene Polynom f noch mit Rest durch das Polynom $g(X):=(X-3)\cdot(X-2)\cdot(X-1)$ dividiert werden.
Die gesuchte Lösung der Interpolationsaufgabe ist:
$f_0(X)=-2\cdot X^2+7\cdot X-4$.

III. Quellen- und Literaturverzeichnis

Skripten: Dr. Folkers
Lineare Algebra, Prof. Schmidt

Internet: www.Hausarbeiten.de