Ganzzahlige Division mit Rest

Für $a, b \in \mathbb{N}$ mit $a \geq b$ gibt es stets eine „Zerlegung“ von a der Form

$$a = q \cdot b + r \text{ mit } 0 \leq r \leq b - 1 \ .$$

Hierbei gilt

$$q = \left\lfloor \frac{a}{b} \right\rfloor$$

(salopp formuliert: b passt q-mal in a rein) und

$$r = a - q \cdot b$$

ist der ganzzahlige Rest.

Zum Beispiel gilt für $a = 99$ und $b = 15$:

$$99 = 6 \cdot 15 + 9 \ .$$

Somit: $q = 6$ und $r = 9$.

Schema des Euklidischen Algorithmus

Berechnung des $\mathrm{ggT}(a_0, a_1)$ durch iterierte ganzzahlige Division mit Rest

a_0	$=$	$q_1 \cdot a_1 + a_2$	a_2	$=$	$-q_1 a_1 + a_0$
a_1	$=$	$q_2 \cdot a_2 + a_3$	a_3	$=$	$-q_2 a_2 + a_1$
	$\ldots$			$\ldots$	
a_i	$=$	$q_{i+1} \cdot a_{i+1} + a_{i+2}$	a_{i+2}	$=$	$-q_{i+1} \cdot q_{i+1} a_{i+1} + a_i$
	$\ldots$			$\ldots$	
a_{k-2}	$=$	$q_{k-1} \cdot a_{k-1} + a_k$	a_k	$=$	$-q_{k-1} \cdot a_{k-1} + a_{k-2}$
a_{k-1}	$=$	$q_k \cdot a_k$			

Es gilt dann

$$\mathrm{ggT}(a_0, a_1) = \mathrm{ggT}(a_1, a_2) = \cdots = \mathrm{ggT}(a_{k-2}, a_{k-1}) = \mathrm{ggT}(a_{k-1}, a_k) = a_k$$

und $a_k = x_i \cdot a_{i+1} + y_i \cdot a_i$ für geeignete $x_i, y_i \in \mathbb{Z}$.

ggT als ganzzahlige Linearkombination

Aus dem Schema des Euklidischen Algorithmus ergibt sich folgende rekursive Berechnung der $x_i, y_i \in \mathbb{Z}$ (zu Herleitung s. unten):

$$x_{k-2} = -q_{k-1} \quad \text{und} \quad y_{k-2} = 1$$

$$x_i = y_{i+1} - x_{i+1} \cdot q_{i+1} \quad \text{und} \quad y_i = x_{i+1}$$

berechnet werden. Insbesondere gilt:

$$\text{ggT}(a_0, a_1) = a_k = x_0 \cdot a_1 + y_0 \cdot a_0 \ .$$

Induktive Herleitung der Rekursionsformel: Aus

$$a_{i+2} = -q_{i+1}a_{i+1} + a_i \text{ und } a_k = x_{i+1}a_{i+2} + y_{i+1}a_{i+1}$$

ergibt sich

$$\begin{aligned} a_k &= x_{i+1}(-q_{i+1}a_{i+1} + a_i) + y_{i+1}a_{i+1} \\ &= \underbrace{(y_{i+1} - q_{i+1}x_{i+1})}_{=:x_i} a_{i+1} + \underbrace{x_{i+1}}_{=:y_i} a_i \ . \end{aligned}$$

Beispiellauf zum erweiterten Euklidischen Algorithmus

Zur Berechnung von ggT$(392, 252)$ erhalten wir mit $a_0 = 392$, $a_1 = 252$ unter Anwendung von

$$x_{k-2} = -q_{k-1} \text{ und } y_{k-2} = 1$$

und

$$x_i = y_{i+1} - x_{i+1}q_{i+1} \text{ und } y_i = x_{i+1}$$

die folgende Rechnung:

i	a_i	a_{i+1}	$q_{i+1} = \lfloor a_i/a_{i+1} \rfloor$	x_i	y_i
0	392	252	1	-3	2
1	252	140	1	2	-1
2	140	112	1	-1	1
3	112	28	4		

Test:

$$28 = \text{ggT}(392, 252) = 2 \cdot 392 - 3 \cdot 252 = 784 - 756$$

kgV-Berechnung
Invertieren modulo m
Simultane Kongruenzen
Restklassenringe
Modulare Arithmetik
Euler'sche Funktion
Sätze von Fermat und Euler

kgv-Berechnung

Aus den Primfaktorzerlegungen

$$a = \prod_{i=1}^{r} p_i^{e_i} \text{ und } b = \prod_{i=1}^{r} p_i^{f_i}$$

mit ganzen Zahlen $e_i, f_i \geq 0$ ergibt sich

$$\text{ggT}(a,b) = \prod_{i=1}^{r} p_i^{\min\{e_i,f_i\}} \text{ und } \text{kgV}(a,b) = \prod_{i=1}^{r} p_i^{\max\{e_i,f_i\}}$$

und somit

$$a \cdot b = \text{ggT}(a,b) \cdot \text{kgV}(a,b) \ .$$

Ein Algorithmus zur Berechnung des ggT liefert damit auch die Berechnung von

$$\text{kgV}(a,b) = \frac{ab}{\text{ggT}(a,b)} \ .$$

(Multiplikative) Invertierbarkeit von zu m teilerfremden Zahlen

Problemstellung:

Gegeben $a \in \mathbb{Z}_m$ mit $\text{ggT}(a, m) = 1$, finde $b \in \mathbb{Z}_m$ mit $ab \equiv 1 \pmod{m}$.

Lösungsmethode:

Bestimme mit dem erweiterten Euklidischen Algorithmus $x, y \in \mathbb{Z}$ mit

$$ax + my = \text{ggT}(a, m) = 1 \ .$$

Hieraus folgt:

$$1 \equiv ax + my \equiv ax + 0 \equiv ax \pmod{m} \ .$$

Setze $b := x \bmod m$.

Nicht-Invertierbarkeit von zu m nicht teilerfremden Zahlen

Betrachte ein $a \in \mathbb{Z}_m$ mit $\text{ggT}(a, m) = d \geq 2$ und setze

$$b = \frac{m}{d} \in \mathbb{Z}_m \setminus \{0\} \text{ und } c = \frac{a}{d} \in \mathbb{Z}_m \ .$$

Dann gilt:

$$a \cdot b \equiv a \cdot \frac{m}{d} \equiv \frac{a}{d} \cdot m \equiv c \cdot m \equiv 0 \pmod{m}$$

Wegen $a \cdot b \equiv 0$ mit $b \not\equiv 0$ heißt a ein „Nullteiler“. Falls zusätzlich $a \not\equiv 0$, dann heißt a ein „nicht-trivialer Nullteiler“.

Ein Nullteiler kann wegen

$$(x \cdot a) \cdot b \equiv x \cdot (a \cdot b) \equiv x \cdot 0 \equiv 0$$

kein Inverses x mit $x \cdot a \equiv 1$ besitzen.

Schlussfolgerung: Ein kleinster Rest modulo m ist genau dann invertierbar, wenn er zu m teilerfremd ist.

Erfüllen simultaner Kongruenzen

Problemstellung: Für paarweise teilerfremde $m_1, \ldots, m_k$ und $m = \prod_{i=1}^{k} m_i$ finde $x \in \mathbb{Z}_m$ mit

$$x \equiv b_1 \pmod{m_1}, \ldots, x \equiv b_k \pmod{m_k} \ .$$

Lösungsmethode:

1. Bestimme $M_i = m/m_i$ und $M_i' = M_i \bmod m_i$ für $i = 1, \ldots, k$. Es gilt: $\mathrm{ggT}(M_i, m_i) = \mathrm{ggT}(M_i', m_i) = 1$ und $M_i \equiv 0 \pmod{m_j}$ für alle $j \neq i$.
2. Bestimme x_i mit $x_i M_i' \equiv 1 \pmod{m_i}$ für $i = 1, \ldots, k$.
   Verwende hierzu den erweiterten Euklidischen Algorithmus oder „Raten und Verifizieren“.
3. Bestimme $u_i = x_i M_i \bmod m$ für $i = 1, \ldots, k$.
   Es gilt: $u_i \equiv 1 \pmod{m_i}$ und $u_i \equiv 0 \pmod{m_j}$ für alle $j \neq i$.
4. Bestimme die Lösung $x = \sum_{i=1}^{k} u_i b_i \bmod m$.

Lösung in $\mathbb{Z}_m$ ist eindeutig ! Warum ?

Chinesischer Restsatz

Für paarweise teilerfremde $m_1, \ldots, m_k$ und $m = \prod_{i=1}^{k} m_i$ gibt es für jede Wahl von

$$b_1 \in \mathbb{Z}_{m_1}, \ldots, b_k \in \mathbb{Z}_{m_k}$$

genau ein $x \in \mathbb{Z}_m$, das die simultanen Kongruenzen

$$x \equiv b_1 \pmod{m_1}, \ldots, x \equiv b_k \pmod{m_k}$$

erfüllt.

Beispiellauf zum Chinesischen Restsatz

Für $m_1 = 8, m_2 = 9, m_3 = 5$ und $m = m_1 m_2 m_3 = 8 \cdot 9 \cdot 5 = 360$ suchen wir nach einem $x \in \mathbb{Z}_m$, das die simultanen Kongruenzen

$$x \equiv 7 \pmod 8,\ x \equiv 1 \pmod 9,\ x \equiv 3 \pmod 5$$

erfüllt. Dazu gehen wir vor wie folgt:

1. $M_1 = m_2 m_3 = 9 \cdot 5 = 45$, $M_2 = m_1 m_3 = 8 \cdot 5 = 40$, $M_3 = m_1 m_2 = 8 \cdot 9 = 72$.
   $M_1' = 45 \bmod 8 = 5$, $M_2' = 40 \bmod 9 = 4$, $M_3' = 72 \bmod 5 = 2$.
2. Wegen $5 \cdot 5 \equiv 1 \pmod 8$, $4 \cdot 7 \equiv 1 \pmod 9$ und $2 \cdot 3 \equiv 1 \pmod 5$ gilt
   $x_1 = 5$, $x_2 = 7$ und $x_3 = 3$.
3. $u_1 = 5 \cdot 45 \bmod 360 = 225$, $u_2 = 7 \cdot 40 \bmod 360 = 280$,
   $u_3 = 3 \cdot 72 \bmod 360 = 216$.
4. $x = 7 \cdot 225 + 1 \cdot 280 + 3 \cdot 216 \bmod 360 = 343$.

Eine Kollektion von abstrakten Rechenregeln

1. $\forall a, b, c \in M : (a + b) + c = a + (b + c)$.
2. $\exists 0 \in M, \forall a \in M : 0 + a = a + 0 = a$.
3. $\forall a \in M, \exists -a \in M : (-a) + a = a + (-a) = 0$.
4. $\forall a, b \in M : a + b = b + a$.
5. $\forall a, b, c \in M : (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
6. $\forall a, b, c \in M : a \cdot (b + c) = a \cdot b + a \cdot c$ und $(b + c) \cdot a = b \cdot a + c \cdot a$.
7. $\exists 1 \in M, \forall a \in M : 1 \cdot a = a \cdot 1 = a$.
8. $\forall a, b \in M : a \cdot b = b \cdot a$.
9. $\forall a \in M \setminus \{0\}, \exists a^{-1} \in M \setminus \{0\} : a^{-1} \cdot a = a \cdot a^{-1} = 1$.

Hierbei steht M für (irgend-)eine Menge mit (irgendwie definierten) binären Operationen „+“ und „·“.

Gruppen, Ringe und Körper

$(M, +)$ ist eine (additive) Gruppe $\Leftrightarrow$ 1.,2.,3.
$(M, +)$ ist eine (additive) abelsche Gruppe $\Leftrightarrow$ 1.,2.,3.,4.
$(M, +, \cdot)$ ist ein Ring $\Leftrightarrow$ 1.,. . .,6.
$(M, +, \cdot)$ ist ein kommutativer Ring mit Einselement $\Leftrightarrow$ 1.,. . .,8.
$(M, +, \cdot)$ ist ein Körper $\Leftrightarrow$ 1.,. . .,9.

Beispiele für kommutative Ringe mit Einselement: $(\mathbb{Z}, +, \cdot)$ und $(\mathbb{Z}_m, +, \cdot)$.

In $(\mathbb{Z}_m, +, \cdot)$ ist für $a \neq 0$ das „additive Inverse“ $-a$ identisch mit $m - a$: $a + (m - a) = m \equiv 0 \pmod{m}$.

Beispiele für Körper: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$.

Prime Restklassen

In $\mathbb{Z}$ gibt es multiplikative Inverse a^{-1} nur für $a \in \{1, -1\}$.

In $\mathbb{Z}_m$ hingegen sind genau die zu m teilerfremden kleinsten Reste invertierbar.

Wir definieren:

$$\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m | \exists x \in \mathbb{Z}_m : a \cdot x \equiv 1 \pmod{m}\} = \{a \in \mathbb{Z}_m | \mathrm{ggT}(a, m) = 1\}$$

Bemerkung $(\mathbb{Z}_m^*, \cdot)$ ist eine (multiplikative) abelsche Gruppe genannt die Gruppe der *primen Restklassen*.

Folgerung: Für eine Primzahl p gilt $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.
Somit ist $(\mathbb{Z}_p, +, \cdot)$ ein Körper.

Beispiel: Prime Restklassen modulo 9

Die Multiplikationstafel für $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ sieht aus wie folgt:

$\cdot$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Es gilt:: $3 \cdot 3 \equiv 6 \cdot 3 \equiv 0 \pmod 9$.

Also sind 3 und 6 in $\mathbb{Z}_9$ nicht-triviale Nullteiler.

Algebraische Struktur der Restklassenringe

Für paarweise teilerfremde $m_1, \ldots, m_k$ und $m = \prod_{i=1}^{k} m_i$ ist Abbildung $h : \mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$, gegeben durch

$$h(a) = (a \bmod m_1, \ldots, a \bmod m_k) \ ,$$

eine Bijektion und erfüllt die „Homomorphiebedingung“

$$h(a+b) = h(a) + h(b) \text{ und } h(a \cdot b) = h(a) \cdot h(b) \ ,$$

d.h., die Ringe $(\mathbb{Z}_m, +, \cdot)$ und $(\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}, +, \cdot)$ sind isomorph (strukturgleich):

$$(\mathbb{Z}_m, +, \cdot) \simeq (\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}, +, \cdot) \ .$$

Analog liefert h eingeschränkt auf $\mathbb{Z}_m^*$ einen Gruppenisomorphismus:

$$(\mathbb{Z}_m^*, \cdot) \simeq (\mathbb{Z}_{m_1}^* \times \cdots \times \mathbb{Z}_{m_k}^*, \cdot) \ .$$

Modulare Arithmetik

Ansatz Sei $m = \prod_{i=1}^{k} m_i$ für paarweise teilerfremde m_i (zum Beispiel die Primzahlpotenzen der Primfaktorzerlegung von m). Rechnen modulo $m_1, \ldots, m_k$ (kleine Zahlen) ist leichter als Rechnen modulo m (große Zahlen). Führe also die Rechnung modulo der m_i aus und übertrage das Ergebnis mit Hilfe des Chinesischen Restsatzes in $\mathbb{Z}_m$.

Beispiel: $m = 360 = 8 \cdot 9 \cdot 5$. Um $199 \cdot 217 \mod 360$ zu berechnen, nutze eine Hilfsabbildung $h : \mathbb{Z}_{360} \to \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$ und gehe vor wie folgt:

1. $199 \overset{h}{\mapsto} (199 \bmod 8, 199 \bmod 9, 199 \bmod 5) = (7, 1, 4)$,
   $217 \overset{h}{\mapsto} (217 \bmod 8, 217 \bmod 9, 217 \bmod 5) = (1, 1, 2)$.
2. $(7, 1, 4) \cdot (1, 1, 2) = (7, 1, 3)$ in $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$.
3. $(7, 1, 3) \overset{h^{-1}}{\mapsto} 343$.
   (Hierzu s. den früheren Beispiellauf zum chinesischen Restsatz.)

Die Euler'sche Funktion

Die Funktion φ, gegeben durch

$$\varphi(m) := |\mathbb{Z}_m^*| \ ,$$

heißt *Euler'sch.*

Für eine Primzahl p gilt $\varphi(p) = p - 1$. Da die nicht zu p teilerfremden Zahlen in $\mathbb{Z}_{p^r}$ gerade die Zahlen $0, p, 2p, \ldots, (p^{r-1} - 1)p$ sind (p^{r-1} viele), gilt

$$\varphi(p^r) = p^r - p^{r-1} = (p-1)p^{r-1} \ .$$

Für m mit Primfaktorzerlegung $m = \prod_{i=1}^{k} p_i^{r_i}$ ergibt sich wegen $(\mathbb{Z}_m^*, \cdot) \simeq (\mathbb{Z}_{p_1^{r_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{m_k}}^*, \cdot)$:

$$\varphi(m) = \prod_{i=1}^{k} \varphi(p_i^{r_i}) = \prod_{i=1}^{k} (p_i - 1)p_i^{r_i - 1} \ .$$

Der kleine Satz von Fermat

Satz (Fermat): $n \geq 2$ ist genau dann eine Primzahl, wenn die Bedingung

$$\forall a \in \mathbb{Z}_n \setminus \{0\} : a^{n-1} \equiv 1 \pmod{n}$$

erfüllt ist.

Der Satz von Euler

Satz (Euler): Für alle $n \geq 2$ und alle $a \in \mathbb{Z}_n^*$ gilt

$$a^{\varphi(n)} \equiv 1 \pmod{n} \ .$$

Folgerung:
Bei einer Potenz modulo n mit einer Basis aus $\mathbb{Z}_n^*$ darf man im Exponenten modulo $\varphi(n)$ rechnen.

Beispiel:
Bei Rechnungen modulo 13 dürfen wir zur Basis 7 im Exponenten modulo 12 rechnen:

$$7^{100} \equiv 7^{100 \bmod 12} \equiv 7^4 \equiv 49 \cdot 49 \equiv 10 \cdot 10 \equiv 100 \equiv 9 \pmod{13} \ .$$