Marko Roczen und Helmut Wolter
unter Mitarbeit von
Wilfred Pohl, Dorin Popescu, Radu Laza

Aufgabensammlung[1]
Lineare Algebra individuell ◁ zur Fundstelle

Aufgabe 1/2/280 (S: Varianten)
Bestimmung von Inversen in Primkörpern (2)

Index: multiplikatives Inverses, Primkörper, Division mit Rest, euklidischer Algorithmus, größter gemeinsamer Teiler, Kettendivision

Stoffeinheiten: 1/2/34 - 1/2/36 Primkörper und Charakteristik

Für Zahlen $f, g \in \mathbb{Z}$, $g \neq 0$ wird die Division mit Rest in der Form

$f : g = q$ Rest r

angegeben, wobei $f = g \cdot q + r$ mit $q, r \in \mathbb{Z}$ und $|\, g \,| > r \geq 0$.
Ausgehend von den Zahlen $r_{-1} := f$, $r_0 := g$, $v_{-1} := 0$, $v_0 := 1$ und mit dem Startindex $i = -1$ führen wir das folgende Verfahren aus:

Berechne {
$i := i + 1$,
$r_{i-1} : r_i = q_{i+1}$ Rest r_{i+1},
falls $\{r_{i+1} \neq 0\}$ $v_{i+1} = v_{i-1} - v_i \cdot q_{i+1}$,
} **solange** $\{r_{i+1} \neq 0\}$,
$k := i$ (letzter Index),
$u_k = (r_k - v_k \cdot g)/f$.

Das Ergebnis des Verfahrens sind die Zahlen r_k, u_k und v_k.

(i) Zeigen Sie, dass r_k der größte gemeinsame Teiler von f und g ist und $u_k \cdot f + v_k \cdot g = r_k$.

(ii) Verwenden Sie das obige Verfahren zur Berechnung des multiplikativen Inversen von 20 im endlichen Primkörper $\mathbb{F}_{29}$.

Lösung. (i) Dass r_k größter gemeinsamer Teiler von f und g ist, folgt aus dem euklidischen Algorithmus, der hier nur um die Berechnung der Zahlen u_k und v_k erweitert wurde (das angegebene Verfahren trägt deshalb auch die Bezeichnung *erweiterter euklidischer Algorithmus*).
Um die Darstellung von r_k als Vielfachensumme zu gewinnen, definieren wir $u_{-1} := 1$ und $u_0 := 0$ sowie mit Hilfe zweier Unbestimmter X und Y die Startgrößen $s_{-1} := u_{-1} \cdot X - v_{-1} \cdot Y$ und $s_0 := u_0 \cdot X - v_0 \cdot Y$ aus $\mathbb{Z}[X, Y]$. Nun kann der vertraute euklidische Algorithmus in jedem Schritt um die Berechnung von

$$s_{i+1} = s_{i-1} - s_i \cdot q_{i+1}$$

erweitert werden; es folgt

[1] Ver. 0.51 (Juli 2004), Institut für Mathematik an der Mathematisch-Naturwissenschaftlichen Fakultät II der Humboldt-Universität zu Berlin, 2004 (Preprint; 2004-17), ISSN 1439-9679
Diese Aufgabensammlung entstand mit teilweiser Förderung durch das Bundesministerium für Bildung und Forschung unter dem Kennzeichen 01NM075D; die Verantwortung für den Inhalt liegt bei den Autoren.
Ähnliche Aufgaben finden Sie im gleichnamigen Internetprojekt Lineare Algebra individuell; als registrierter Nutzer können Sie dort online Aufgaben erzeugen und Lehrstoff nach eigenem Wunsch zusammenstellen lassen.

$$s_{i+1} = u_{i+1}\cdot X - v_{i+1}\cdot Y = (u_{i-1} - u_i\cdot q_{i+1})\cdot X - (v_{i-1} - v_i\cdot q_{i+1})\cdot Y\,.$$

Mit $X = f$ und $Y = g$ gilt $s_i = r_i$. Für alle Reste r_i ist damit eine Darstellung als Vielfachensumme der Ausgangszahlen gewonnen.
Der Kunstgriff und Vorteil des vorliegenden Verfahrens besteht darin, nur die Zahlen v_i zu berechnen; u_k kann dann im letzten Schritt durch Division erhalten werden.

(ii) Das Verfahren ist gut geeignet zur Inversenberechnung in einem endlichen Primkörper. Wir initialisieren r_{-1} mit der Primzahl p und r_0 mit der zu invertierenden Zahl z. Das Verfahren liefert

$$u_k\cdot p + v_k\cdot z = 1.$$

Es folgt $z^{-1} = v_k$ in $\mathbb{F}_p$ (vgl. 1/2/29). Auf die Berechnung von u_k kann hier verzichtet werden.
Um das multiplikative Inverse von 20 in $\mathbb{F}_{29}$ zu bestimmen, wird also

$$r_{-1} = 29,\ r_0 = 20$$

initialisiert. Es entsteht die Tabelle:

$29 : 20 = 1$ Rest 9	$v_{-1} - 1\cdot v_0 = v_1$	$v_1 = -1$
$20 : \ 9 = 2$ Rest 2	$v_0 \ - 2\cdot v_1 = v_2$	$v_2 = 3$
$9 : \ 2 = 4$ Rest 1	$v_1 \ - 4\cdot v_2 = v_3$	$v_3 = -13$

Wir erhalten als Resultat $20^{-1} = -13$ im Körper $\mathbb{F}_{29}$.