

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

Aufgabensammlung¹

Lineare Algebra individuell

◀ zur Fundstelle

Aufgabe 1/2/275

(S: Varianten)

Bestimmung von Inversen in Primkörpern (1)

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

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

Bestimmen Sie das multiplikative Inverse der Zahl 16 im endlichen Primkörper $\mathbb{F}_{23}$.

Lösung. Der größte gemeinsame Teiler von $f = 23$ und $g = 16$ ist 1, denn f ist Primzahl. Wir stellen 1 als Vielfachensumme von f und g dar. Dazu setzen wir $r_{-1} := f$ und $r_0 := g$. Für $i > 0$ wird mit r_i der Rest bei der i -ten Division bezeichnet. Es ergibt sich die folgende Tabelle:

$23 : 16 = 1 \text{ Rest } 7$	$r_{-1} - 1 \cdot r_0 = r_1$	$r_1 = f - g$
$16 : 7 = 2 \text{ Rest } 2$	$r_0 - 2 \cdot r_1 = r_2$	$r_2 = -2f + 3g$
$7 : 2 = 3 \text{ Rest } 1$	$r_1 - 3 \cdot r_2 = r_3$	$r_3 = 7f - 10g$

Die erste Spalte enthält den euklidischen Algorithmus (vgl. 1/2/26). In der zweiten Spalte sind die Rekursionen der Reste angegeben. Die letzte Spalte der Tabelle entsteht aus der zweiten durch Einsetzen der bereits bekannten Ausdrücke und enthält die Darstellung der Reste als Vielfachensummen. Der größte gemeinsame Teiler ist $r_3 = 1$; er ergibt sich als Vielfachensumme

$$1 = 7f - 10g.$$

Bei Übergang zu den Restklassen verschwindet der erste Summand und es folgt in $\mathbb{F}_{23}$ (vgl. 1/2/29)

$$-10 = 16^{-1}.$$

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.