Erweiterter EUKLIDischer Algorithmus

Es seien $a, b \in N^*$, $a > b$.

Man bilde die (endlichen) Folgen (r_n), (x_n) und (y_n):

$\boxed{r_0 = b,\ r_1 = \mathrm{mod}(a,b),\ r_2 = \mathrm{mod}(r_0, r_1),\ \ldots,\ r_n = \mathrm{mod}(r_{n-2}, r_{n-1}),}$

Abbruch falls $r_n = 0$.

$x_0 = 0,\ x_1 = 1,\quad x_2 = x_0 - q_2 x_1,\ \ldots,\ x_j = x_{j-2} - q_j x_{j-1}\quad (j \le n-1),$

$y_0 = 1,\ y_1 = -q_1,\ y_2 = y_0 - q_2 y_1,\ \ldots,\ y_j = y_{j-2} - q_j y_{j-1}\quad (j \le n-1).$

Dabei ist q_j der Quotient bei der Division von r_{j-2} durch r_{j-1},

d.h. $r_{j-2} = q_j r_{j-1} + r_j$.

Dann gilt $\boxed{ggT(a, b) = r_{n-1}}$ (letzter nicht verschwindender Rest), ferner gilt

$r_j = x_j \cdot a + y_j \cdot b$ (j = 1, … , n–1) also $\boxed{ggT(a,b) = x_{n-1} \cdot a + y_{n-1} \cdot b}$ (*).

Ermittlung der modularen Inversen von c zum teilerfremden Modul m (c < m)

Der erweiterte Euklidische Algorithmus (mit a = m, b = c) liefert eine Darstellung der Gestalt $\boxed{1 = x \cdot m + y \cdot c}$, vgl. (*). Damit gilt $y \cdot c \equiv 1 \pmod m$ und damit

$c^{-1} \equiv y \pmod m$ (Falls y nicht in Z_m liegt, muss der zu y kongruente Wert aus Z_m gebildet werden!)

Vorlesungsbeispiel: Man ermittle die modulare Inverse von 11 zum Modul 25.
Bezeichnungen a := 25, b := 11

Rechenschema 1:

$r_{j-2} : r_{j-1} = q_j$ Rest r_j	$r_j = r_{j-2} - q_j \cdot r_{j-1}$	$r_j = x_j \cdot a + y_j \cdot b$	
		$11 = 0 \cdot 25 + 1 \cdot 11$	(0)
25 : 11 = 2 Rest 3	$3 = 25 - 2 \cdot 11$ →	$3 = 1 \cdot 25 - 2 \cdot 11$	(1)
11 : 3 = 3 Rest 2	$2 = 11 - 3 \cdot 3$	$2 = -3 \cdot 25 + 7 \cdot 11$	(2)
3 : 2 = 1 Rest 1	$1 = 3 - 1 \cdot 2$	$1 = 4 \cdot 25 - 9 \cdot 11$	(3)
[2 : 1 = 2 Rest 0]			

Aus (3) folgt $11^{-1} \equiv -9 \equiv \underline{\underline{16}} \pmod{25}$.

<u>Bemerkungen zur letzten Spalte des Rechenschemas 1:</u>

Zeile (0): Stets die kleinere der beiden Zahlen (hier b = 11) als triviale Linearkombination (hier 11 = 0 · 25 + 1 · 11) darstellen!

Zeile (1): Stets Linearkombination aus dem links stehenden Feld übernehmen!

<u>Zeile (2):</u> Linksstehende Gleichung unter Verwendung der beiden darüber stehenden Felder als Linearkombination von a und b schreiben:

$2 = 11 - 3 \cdot 3 = \boxed{0 \cdot 25 + 1 \cdot 11} - 3 \cdot \boxed{(1 \cdot 25 - 2 \cdot 11)} = -3 \cdot 25 + 7 \cdot 11$, analog

<u>Zeile (3):</u> $1 = 3 - 2 = 1 \cdot 25 - 2 \cdot 11 - (-3 \cdot 25 + 7 \cdot 11) = 4 \cdot 25 - 9 \cdot 11$.

Die Rechnung lässt sich verkürzt schreiben. Für die modulare Inverse wird nur y_{n-1} benötigt, d.h., ausgehend vom einfachen Algorithmus wird folgende Rekursion durchgeführt:

$$y_o = 1,\ y_1 = -q_1,\ y_2 = y_o - q_2 y_1,\ \ldots,\ y_j = y_{j-2} - q_j y_{j-1} \quad (j \le n-1)\,.$$

Damit ergibt sich das Rechenschema 2:

j	$r_{j-2} : r_{j-1} = q_j$ Rest r_j	y_j
0		1
1	25 : 11 = 2 Rest 3	–2
2	11 : 3 = 3 Rest 2	7
3	3 : 2 = 1 Rest 1	–9
[4]	[2 : 1 = 2 Rest 0]	

Kommentar zur letzten Spalte:

$y_0 = 1$ und $y_1 = -q_1 = -2$ ergeben sich aus den Anfangsbedingungen,

$y_2 = y_0 - q_2 \cdot y_1 = 1 - 3 \cdot (-2) = 7$ und $y_3 = y_1 - q_3 \cdot y_2 = -2 - 1 \cdot 7 = -9$ aus der Rekursionsformel $y_j = y_{j-2} - q_j y_{j-1}$.

Aus Zeile j = 3 (Rest = 1) ergibt sich die gesuchte modulare Inverse

$$11^{-1} \equiv y_3 = -9 \equiv \underline{\underline{16}} \pmod{25}.$$

(Falls y nicht in Z_m liegt, muss der zu y kongruente Wert aus Z_m gebildet werden!)

Bemerkungen:

Rechenschema 1 ist zwar umfangreicher, hat aber den Vorteil, dass in jedem Schritt eine Rechenkontrolle (in der 3. Spalte!) möglich ist. Für die Lösung spezieller diophantischer Gleichungen (Gleichungen mit ganzzahligen Koeffizienten, bei denen nur ganzzahlige Lösungen von Interesse sind), vgl. etwa die Übungsaufgabe A2.3 ist auch der Wert x_{n-1} wichtig, also ist hier ebenfalls das Schema 1 zweckmäßig.