S. Wewers, S. Wilke

Kryptographie, SS 06

Lösung 1

Aufgabe 1.

(a) Gesucht: ggT(291, 201)
Anwenden des erweiterten euklidischen Algorithmus liefert:

k	0	1	2	3	4	5	6
r_k	291	201	90	21	6	3	0
q_k		1	2	4	3	2	
x_k	1	0	1	2	9	29	
y_k	0	1	1	3	13	42	

Damit ist $\text{ggT}(291, 201) = 3 = -29 \cdot 291 + 42 \cdot 201$

(b) Gesucht: ggT(1428, 882)
Anwenden des erweiterten euklidischen Algorithmus liefert:

k	0	1	2	3	4	5	6	7	8
r_k	1428	882	546	336	210	126	84	42	0
q_k		1	1	1	1	1	1	2	
x_k	1	0	1	1	2	3	5	8	
y_k	0	1	1	2	3	5	8	13	

Damit ist $\text{ggT}(1428, 882) = 42 = -8 \cdot 1428 + 13 \cdot 882$.

Aufgabe 2.

(a) $12 = 4001 \cdot x + 2689 \cdot y$
Wir setzen an mit dem erweiterten euklidischen Algorithmus:

k	0	1	2	3	4	5	6
r_k	4001	2689	1312	65	12	5	$\cdots$
q_k		1	2	20	5	$\cdots$	
x_k	1	0	1	2	41	$\cdots$	
y_k	0	1	1	3	61	$\cdots$	

Nach Schritt 4 erhalten wir somit eine ganzzahlige Linearkombination von 12 aus 4001 und 2689; nämlich $12 = 41 \cdot 4001 - 61 \cdot 2689$, also $x = 41$, $y = -61$. Wir können den euklidischen Algorithmus also abbrechen. Führt man ihn bis zum Ende durch, erhält man übrigens

$$\text{ggT}(4001, 2689) = 1 = -1117 \cdot 4001 + 1662 \cdot 2689,$$

und damit

$$x = -1117 \cdot 12 = -13404 \text{ und } y = 1662 \cdot 12 = 19944.$$

(b) $24 = 30128 \cdot x + 4249 \cdot y$
Wir setzen erneut mit dem erweiterten euklidischen Algorithmus an.

k	0	1	2	3	4	5
r_k	30128	4249	385	14	7	0
q_k		7	11	27	2	
x_k	1	0	1	11	$\cdots$	
y_k	0	1	7	78	$\cdots$	

Nach Schritt 3 erkennt man $\text{ggT}(30128, 4249) = \text{ggT}(14, 7) = 7$. Es gilt aber $7 \nmid 24$, also ist $24 = 30128x + 4249y$ nicht lösbar mit $x, y \in \mathbb{Z}$. Die Berechnung der letzten x_k, y_k erübrigt sich damit.

(c) $42 = 291 \cdot x + 201 \cdot y$
Aus 1a) wissen wir $3 = -29 \cdot 291 + 42 \cdot 201$ und damit

$$42 = (-29 \cdot 14) \cdot 291 + (42 \cdot 14) \cdot 201,$$

also $x = -406$ und $y = 588$.

Aufgabe 3. $1 = 143 \cdot x + 187 \cdot y + 221 \cdot z$
Wir wenden zunächst den erweiterten euklidischen Algorithmus an für 187 und 221:

k	0	1	2	3	4
r_k	221	187	34	17	0
q_k		1	5	2	
x_k	1	0	1	5	
y_k	0	1	1	6	

Wir erhalten also $\text{ggT}(221, 187) = 17 = -5 \cdot 221 + 6 \cdot 187$. Jetzt wenden wir den euklidischen Algorithmus erneut an auf 143 und 17 und erhalten:

k	0	1	2	3	4	5
r_k	143	17	7	3	1	0
q_k		8	2	2	3	
x_k	1	0	1	2	5	
y_k	0	1	8	17	42	

Also ist

$$\begin{aligned} 1 &= \text{ggT}(143, 17) = \text{ggT}(143, \text{ggT}(221, 187)) = \text{ggT}(143, 187, 221) \\ &= 5 \cdot 143 - 42 \cdot 17 = 5 \cdot 143 - 42 \cdot (-5 \cdot 221 + 6 \cdot 187). \end{aligned}$$

Wir erhalten also $x = 5$, $y = -42 \cdot 6 = -252$, $z = -42 \cdot -5 = 210$.