Universität Siegen
Lehrstuhl Theoretische Informatik

Carl Philipp Reh
Daniel König

Diskrete Mathematik für Informatiker

WS 2016/2017

Übung 11

1. Berechnen Sie mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler der Zahlen m und n ($\text{ggT}(m, n)$) und geben Sie den $\text{ggT}(m, n)$ als Linearkombination von m und n an ($\text{ggT}(m, n) = x \cdot m + y \cdot n$ mit $x, y \in \mathbb{Z}$):

   a) $m = 18$, $n = 30$

   b) $m = 34$, $n = 55$

   c) $m = 810$, $n = 2008$

2. Berechnen Sie die folgenden Werte der eulerschen Funktion:

   a) $\varphi(9)$

   b) $\varphi(35)$

   c) $\varphi(143)$

   d) $\varphi(1024)$

3. Finden Sie $x \in \mathbb{Z}_{210}$ mit den Bedingungen:

   $1 = x \bmod 3$

   $3 = x \bmod 7$

   $5 = x \bmod 10$

4. 17 chinesische Piraten erbeuten eine Truhe mit Goldstücken. Beim Versuch, diese gleichmäßig zu verteilen, bleiben 7 Goldstücke übrig. Um diese entbrennt ein heftiger Streit, bei dem einer der Piraten das Leben lässt. Die verbleibenden 16 Piraten versuchen erneut, die Goldstücke gerecht zu verteilen, behalten jedoch 11 Stücke übrig. Bei der folgenden Auseinandersetzung geht wieder einer der Streitenden über Bord. Den 15 Überlebenden gelingt dann die Teilung. Wie viele Goldstücke müssen es mindestens gewesen sein?

Lösung zu Übung 11

1. Zur Erinnerung: Wir suchen ein Paar $(x, y) \in \mathbb{Z}^2$ mit

$$\text{ggT}(m, n) = x \cdot m + y \cdot n.$$

Ein rekursiver Aufruf von EUKLID$(n \bmod m, m)$ liefert ein Paar $(x', y') \in \mathbb{Z}^2$ so, dass gilt

$$\text{ggT}(n \bmod m, m) = x' \cdot (n \bmod m) + y' \cdot m.$$

Damit erhalten wir

$$\begin{aligned}\text{ggT}(n \bmod m, m) &= x' \cdot (n \bmod m) + y' \cdot m \\ &= x' \cdot (n - (n \operatorname{div} m) \cdot m) + y' \cdot m \\ &= x' \cdot n - x' \cdot (n \operatorname{div} m) \cdot m + y' \cdot m \\ &= x' \cdot n + (y' - x' \cdot (n \operatorname{div} m)) \cdot m.\end{aligned}$$

Zusammen mit der Tatsache, dass $\text{ggT}(m, n) = \text{ggT}(n \bmod m, m)$, sind die Faktoren x und y gefunden:

$$\begin{aligned}y &= x', \\ x &= y' - x' \cdot (n \operatorname{div} m).\end{aligned}$$

a)

m	n	$n \operatorname{div} m$	$n \bmod m$	x	y
18	30	1	12	2	-1
12	18	1	6	-1	1
6	12	2	0	1	0

b)

m	n	$n \operatorname{div} m$	$n \bmod m$	x	y
34	55	1	21	-21	13
21	34	1	13	13	-8
13	21	1	8	-8	5
8	13	1	5	5	-3
5	8	1	3	-3	2
3	5	1	2	2	-1
2	3	1	1	-1	1
1	2	2	0	1	0

c)

m	n	$n \operatorname{div} m$	$n \bmod m$	x	y
810	2008	2	388	-295	119
388	810	2	34	119	-57
34	388	11	14	-57	5
14	34	2	6	5	-2
6	14	2	2	-2	1
2	6	3	0	1	0

2. a) $\varphi(9) = |\{1, 2, 4, 5, 7, 8\}| = 6$

   b) $\varphi(35) = \varphi(5 \cdot 7) = (5-1)(7-1) = 4 \cdot 6 = 24$

   c) $\varphi(143) = \varphi(11 \cdot 13) = (11-1)(13-1) = 10 \cdot 12 = 120$

   d) $\varphi(1024) = |\{1 \leq x < 1024 \mid x \text{ ungerade } \}| = 512$

3. Wir wenden den Chinesischen Restsatz an. Aus der Aufgabe haben wir $m_1 = 3$, $m_2 = 7$, $m_3 = 10$, $a_1 = 1$, $a_2 = 3$ und $a_3 = 5$. Daraus ergeben sich zunächst $M = m_1 m_2 m_3 = 210$, $M_1 = M/m_1 = 70$, $M_2 = M/m_2 = 30$ und $M_3 = M/m_3 = 21$. Nun bestimmen wir N_1, N_2 und N_3:

   EUKLID(m_1, M_1)**:**

m	n	$n \operatorname{div} m$	$n \bmod m$	x	y
3	70	23	1	-23	1
1	3	3	0	1	0

   EUKLID(m_2, M_2)**:**

m	n	$n \operatorname{div} m$	$n \bmod m$	x	y
7	30	4	2	13	-3
2	7	3	1	-3	1
1	2	2	0	1	0

   EUKLID(m_3, M_3)**:**

m	n	$n \operatorname{div} m$	$n \bmod m$	x	y
10	21	2	1	-2	1
1	10	10	0	1	0

   und erhalten $N_1 = 1$, $N_2 = -3$ und $N_3 = 1$.

Insgesamt haben wir also:

$$\begin{aligned} x &= \sum_{i=1}^{3} a_i N_i M_i \bmod M \\ &= 1 \cdot 1 \cdot 70 + 3 \cdot (-3) \cdot 30 + 5 \cdot 1 \cdot 21 \bmod 210 \\ &= 70 - 270 + 105 \bmod 210 \\ &= -95 \bmod 210 \\ &= 115 \end{aligned}$$

4. Aus der Aufgabenstellung lesen wir folgende Bedinungen für die Anzahl x der Goldstücke:

$$\begin{aligned} 11 &= x \bmod 16 \\ 7 &= x \bmod 17 \end{aligned}$$

Wir wenden erneut den Chinesischen Restsatz an, wobei $m_1 = 16$, $m_2 = 17$, $a_1 = 11$ und $a_2 = 7$. Damit erhalten wir $M = m_1 m_2 = 16 \cdot 17 = 272$, $M_1 = M/m_1 = 17$ und $M_2 = M/m_2 = 16$. Nun bestimmen wir N_1 und N_2:

EUKLID(m_1, M_1)**:**

m	n	$n \operatorname{div} m$	$n \bmod m$	x	y
16	17	1	1	-1	1
1	16	16	0	1	0

EUKLID(m_2, M_2)**:** Da $m_2 > M_2$, berechnen wir stattdessen EUKLID(M_2, m_2):

m	n	$n \operatorname{div} m$	$n \bmod m$	x	y
16	17	1	1	-1	1
1	16	16	0	1	0

Das Ergebnis N_2 wird dann entsprechend aus der x-Spalte abgelesen.

Insgesamt erhalten wir $N_1 = 1$ und $N_2 = -1$, und damit

$$\begin{aligned} x &= \sum_{i=1}^{2} a_i N_i M_i \bmod M \\ &= 11 \cdot 1 \cdot 17 + 7 \cdot (-1) \cdot 16 \bmod 272 \\ &= 75 \bmod 272 \\ &= 75 \end{aligned}$$