Lösungen Blatt 5, Mathematik für Informatiker 1[*]

AUFGABE 1. Ein Student möchte in die USA reisen und wechselt ganzzahlige Beträge von Euro und Schweizer Franken in US-Dollar. Die Wechselkurse sind $\$\,1.35 = €\,1.00$ und $\$\,1.12 =$ CHF 1.00. Wenn der Student insgesamt $\$\,66.49$ erhält, wieviel Geld von jeder Währung wurde gewechselt? (Hinweis: Lösen Sie die entsprechende Diophantische Gleichung beispielsweise mit Hilfe des erweiterten Euklidischen Algorithmus!)

Lösung. Die zu lösende Diophantische Gleichung lautet (nach Multiplikation mit 100)

$$135x + 112y = 6649, \tag{1}$$

wobei $x \in \mathbb{N}_0$ die Anzahl der Euros und $y \in \mathbb{N}_0$ die Anzahl der Schweizer Franken ist. Wegen $135 = 3^3 \cdot 5$ und $112 = 2^4 \cdot 7$ gilt $\mathrm{ggT}(135, 112) = 1$. Somit besitzt die Gleichung (1) wenigstens eine Lösung $(x, y) \in \mathbb{Z}^2$. Um eine solche Lösung zu berechnen, verschaffen wir uns zuerst mit Hilfe des erweiterten Euklidischen Algorithmus eine Lösung $(\hat{x}, \hat{y}) \in \mathbb{Z}^2$ der Gleichung

$$135\hat{x} + 112\hat{y} = \mathrm{ggT}(135, 112) = 1. \tag{2}$$

Wir starten mit $\hat{r}_0 = 135$, $\hat{x}_0 = 1$, $\hat{y}_0 = 0$ sowie $\hat{r}_1 = 112$, $\hat{x}_1 = 0$, $\hat{y}_1 = 1$ und erhalten für $k = 2$

$$\begin{aligned} \hat{r}_2 &= \hat{r}_0 \bmod \hat{r}_1 = 135 \bmod 112 = 23, & \hat{q}_2 &= \hat{r}_0 \operatorname{div} \hat{r}_1 = 135 \operatorname{div} 112 = 1, \\ \hat{x}_2 &= \hat{x}_0 - \hat{q}_2\hat{x}_1 = 1 - 1 \cdot 0 = 1, & \hat{y}_2 &= \hat{y}_0 - \hat{q}_2\hat{y}_1 = 0 - 1 \cdot 1 = -1. \end{aligned}$$

Für $k = 3$ ergibt sich

$$\begin{aligned} \hat{r}_3 &= \hat{r}_1 \bmod \hat{r}_2 = 112 \bmod 23 = 20, & \hat{q}_3 &= \hat{r}_1 \operatorname{div} \hat{r}_2 = 112 \operatorname{div} 23 = 4, \\ \hat{x}_3 &= \hat{x}_1 - \hat{q}_3\hat{x}_2 = 0 - 4 \cdot 1 = -4, & \hat{y}_3 &= \hat{y}_1 - \hat{q}_3\hat{y}_2 = 1 + 4 \cdot 1 = 5. \end{aligned}$$

Für $k = 4$ setzen wir fort mit

$$\begin{aligned} \hat{r}_4 &= \hat{r}_2 \bmod \hat{r}_3 = 23 \bmod 20 = 3, & \hat{q}_4 &= \hat{r}_2 \operatorname{div} \hat{r}_3 = 23 \operatorname{div} 20 = 1, \\ \hat{x}_4 &= \hat{x}_2 - \hat{q}_4\hat{x}_3 = 1 + 1 \cdot 4 = 5, & \hat{y}_4 &= \hat{y}_2 - \hat{q}_4\hat{y}_3 = -1 - 1 \cdot 5 = -6. \end{aligned}$$

Für $k = 5$ folgt daraus

$$\begin{aligned} \hat{r}_5 &= \hat{r}_3 \bmod \hat{r}_4 = 20 \bmod 3 = 2, & \hat{q}_5 &= \hat{r}_3 \operatorname{div} \hat{r}_4 = 20 \operatorname{div} 3 = 6, \\ \hat{x}_5 &= \hat{x}_3 - \hat{q}_5\hat{x}_4 = -4 - 6 \cdot 5 = -34, & \hat{y}_5 &= \hat{y}_3 - \hat{q}_5\hat{y}_4 = 5 + 6 \cdot 6 = 41. \end{aligned}$$

Für $k = 6$ ergibt sich

$$\begin{aligned} \hat{r}_6 &= \hat{r}_4 \bmod \hat{r}_5 = 3 \bmod 2 = 1, & \hat{q}_6 &= \hat{r}_4 \operatorname{div} \hat{r}_5 = 3 \operatorname{div} 2 = 1, \\ \hat{x}_6 &= \hat{x}_4 - \hat{q}_6\hat{x}_5 = 5 + 1 \cdot 34 = 39, & \hat{y}_6 &= \hat{y}_4 - \hat{q}_6\hat{y}_5 = -6 - 1 \cdot 41 = -47. \end{aligned}$$

[*]Mit der Bitte um Entschuldigung für das Durcheinander.

Schließlich erreichen wir für $k = 7$ das Abbruchkriterium $\hat{r}_7 = \hat{r}_5 \bmod \hat{r}_6 = 2 \bmod 1 = 0$. Damit löst $(\hat{x}, \hat{y}) = (\hat{x}_6, \hat{y}_6) = (39, -47) \in \mathbb{Z}^2$ die Gleichung (2).

Wegen $\mathrm{ggT}(135, 112) = 1$ haben somit alle Lösungen $(x, y) \in \mathbb{Z}^2$ der Diophantische Gleichung (1) die Gestalt

$$(x, y) = (6649\hat{x} + 112k, 6649\hat{y} - 135k) = (259311 + 112k, -312503 - 135k) \quad \text{für } k \in \mathbb{Z}.$$

Die Lösung $(x, y) \in \mathbb{N}_0 \times \mathbb{N}_0$ ergibt sich wegen $259311 \operatorname{div} 112 = 2315$ und $312503 \operatorname{div} 135 = 2314$ für $k = -2315$, also $(x, y) = (31, 22)$. Damit wurden Beträge von € 31 sowie CHF 22 in $ 66.49 umgetauscht. □

Aufgabe 2. Sei das Alphabet fortlaufend mit den Zahlen $0, \ldots, 25$ identifiziert. Um einen Klartext mittels RSA zu verschlüsseln, werden die Primzahlen $p = 53$ und $q = 13$ gewählt. Zusätzlich wird die Zahl $e = 11$ genutzt.

a) Generieren Sie den öffentlichen Schlüssel und kodieren Sie den Klartext `GEDULD`!

b) Dekodieren Sie die Zeichenkette `647 031 670 093 050 031 661`!

Proof. a) Es gilt $n = p \cdot q = 689$. Damit ist der öffentliche Schlüssel $(e, n) = (11, 689)$. Für die Zahl $m = (p-1) \cdot (q-1) = 624$ gilt $\mathrm{ggT}(e, m) = (11, 624) = 1$. Der gegebene Klartext `GEDULD` wird mit Hilfe der Kodierungssvorschrift $y = x^e \bmod n = x^{11} \bmod 689$ verschlüsselt:

Klartext	G	E	D	U	L	D
x	06	04	03	20	11	03
y	661	361	074	171	643	074

b) Um Zeichenketten dekodieren zu können, wird zunächst das multiplikative Inverse d von $e = 11$ in $\mathbb{Z}_m$ für $m = (p-1) \cdot (q-1) = 624$ mit Hilfe der Lösung $(\hat{x}, \hat{y}) \in \mathbb{Z}^2$ der Gleichung

$$11\hat{x} + 624\hat{y} = \mathrm{ggT}(11, 624) = 1$$

unter Benutzung des erweiterten Euklidischen Algorithmus berechnet: Wir starten mit den Werten $\hat{r}_0 = 11$, $\hat{x}_0 = 1$, $\hat{y}_0 = 0$ und $\hat{r}_1 = 624$, $\hat{x}_1 = 0$, $\hat{y}_1 = 1$ und erhalten für $k = 2$

$$\begin{aligned} \hat{r}_2 &= \hat{r}_0 \bmod \hat{r}_1 = 11 \bmod 624 = 11, & \hat{q}_2 &= \hat{r}_0 \operatorname{div} \hat{r}_1 = 11 \operatorname{div} 624 = 0, \\ \hat{x}_2 &= \hat{x}_0 - \hat{q}_2\hat{x}_1 = 1 - 0 \cdot 0 = 1, & \hat{y}_2 &= \hat{y}_0 - \hat{q}_2\hat{y}_1 = 0 - 0 \cdot 1 = 0. \end{aligned}$$

Für $k = 3$ ergibt sich

$$\begin{aligned} \hat{r}_3 &= \hat{r}_1 \bmod \hat{r}_2 = 624 \bmod 11 = 8, & \hat{q}_3 &= \hat{r}_1 \operatorname{div} \hat{r}_2 = 624 \operatorname{div} 11 = 56, \\ \hat{x}_3 &= \hat{x}_1 - \hat{q}_3\hat{x}_2 = 0 - 56 \cdot 1 = -56, & \hat{y}_3 &= \hat{y}_1 - \hat{q}_3\hat{y}_2 = 1 - 56 \cdot 0 = 1. \end{aligned}$$

Für $k = 4$ setzen wir fort mit

$$\hat{r}_4 = \hat{r}_2 \bmod \hat{r}_3 = 11 \bmod 8 = 3, \quad \hat{q}_4 = \hat{r}_2 \operatorname{div} \hat{r}_3 = 11 \operatorname{div} 8 = 1,$$
$$\hat{x}_4 = \hat{x}_2 - \hat{q}_4\hat{x}_3 = 1 + 1 \cdot 56 = 57, \quad \hat{y}_4 = \hat{y}_2 - \hat{q}_4\hat{y}_3 = 0 - 1 \cdot 1 = -1.$$

Für $k = 5$ erhält man

$$\hat{r}_5 = \hat{r}_3 \bmod \hat{r}_4 = 8 \bmod 3 = 2, \qquad \hat{q}_5 = \hat{r}_3 \operatorname{div} \hat{r}_4 = 8 \operatorname{div} 3 = 2,$$
$$\hat{x}_5 = \hat{x}_3 - \hat{q}_5\hat{x}_4 = -56 - 2 \cdot 57 = -170, \quad \hat{y}_5 = \hat{y}_3 - \hat{q}_5\hat{y}_4 = 1 + 2 \cdot 1 = 3.$$

Für $k = 6$ ergibt sich

$$\hat{r}_6 = \hat{r}_4 \bmod \hat{r}_5 = 3 \bmod 2 = 1, \qquad \hat{q}_6 = \hat{r}_4 \operatorname{div} \hat{r}_5 = 3 \operatorname{div} 2 = 1,$$
$$\hat{x}_6 = \hat{x}_4 - \hat{q}_6\hat{x}_5 = 57 + 1 \cdot 170 = 227, \quad \hat{y}_6 = \hat{y}_4 - \hat{q}_6\hat{y}_5 = -1 - 1 \cdot 3 = -4.$$

Schließlich erreichen wir für $k = 7$ das Abbruchkriterium $\hat{r}_7 = \hat{r}_5 \bmod \hat{r}_6 = 2 \bmod 1 = 0$. Damit löst $(\hat{x}, \hat{y}) = (\hat{x}_6, \hat{y}_6) = (227, -4) \in \mathbb{Z}^2$ die Gleichung $11\hat{x} + 624\hat{y} = 1$, und wir erhalten das multiplikative Inverse $d = 11^{-1} = 227 \bmod 624 = 227$ in $\mathbb{Z}_{624}$. Die gegebene Zeichenkette `647 031 670 093 050 031 661` kann nun mit der Dekodierungssvorschrift $x = y^d \bmod n = y^{227} \bmod 689$ entschlüsselt werden: Etwa

$$x = 647^{227} \bmod 689 = 17 \quad \text{usw.}$$

Ein Quell-Code (Fortran) hierzu fuer $y = 647$:

```
      implicit none
      integer ell, d, n, x, y
c
      d = 227
      n = 689
      y = 647
c
      x = 1
c
      do ell = 1, d
         x = x*y
  100    if (x .ge. n) then
            x = x - n
            goto 100
         end if
         write(*,*) ell, x
      end do
      end
```

Analog fuer $y = 031, 670, ...$ usw. Das Ergebnis ist:

y	647	031	670	093	050	031	661
x'	17	08	02	07	19	08	06
Klartext	R	I	C	H	T	I	G

□

Aufgabe 3.

a) Finden Sie alle Lösungen $x \in \mathbb{Z}_{33}$ der Kongruenz

$$28x \equiv 119 \,(\text{mod } 33).$$

b) Berechnen Sie $x = 3^{10} \bmod 11$ in $\mathbb{Z}_{11}$ und $y = 2^{12} \bmod 13$ in $\mathbb{Z}_{13}$ mit Hilfe des *Kleinen Satzes von Fermat* aus der Vorlesung!

Lösung. a) Wegen $\text{ggT}(28, 33) = 1$ hat 28 hat ein multiplikatives Inverses in $\mathbb{Z}_{33}$. Zur Berechnung suchen wir eine Lösung $(\hat{x}, \hat{y}) \in \mathbb{Z}^2$ der Gleichung $33\hat{x} + 28\hat{y} = 1$ mit Hilfe des erweitertern Euklidischen Algorithmus: Wir starten mit $\hat{r}_0 = 33$, $\hat{x}_0 = 1$, $\hat{y}_0 = 0$ und $\hat{r}_1 = 28$, $\hat{x}_1 = 0$, $\hat{y}_1 = 1$ und erhalten für $k = 2$ zunächst

$$\begin{aligned} \hat{r}_2 &= \hat{r}_0 \bmod \hat{r}_1 = 33 \bmod 28 = 5, & \hat{q}_2 &= \hat{r}_0 \operatorname{div} \hat{r}_1 = 33 \operatorname{div} 28 = 1, \\ \hat{x}_2 &= \hat{x}_0 - \hat{q}_2\hat{x}_1 = 1 - 1 \cdot 0 = 1, & \hat{y}_2 &= \hat{y}_0 - \hat{q}_2\hat{y}_1 = 0 - 1 \cdot 1 = -1. \end{aligned}$$

Für $k = 3$ ergibt sich

$$\begin{aligned} \hat{r}_3 &= \hat{r}_1 \bmod \hat{r}_2 = 28 \bmod 5 = 3, & \hat{q}_3 &= \hat{r}_1 \operatorname{div} \hat{r}_2 = 28 \operatorname{div} 5 = 5, \\ \hat{x}_3 &= \hat{x}_1 - \hat{q}_3\hat{x}_2 = 0 - 5 \cdot 1 = -5, & \hat{y}_3 &= \hat{y}_1 - \hat{q}_3\hat{y}_2 = 1 + 5 \cdot 1 = 6. \end{aligned}$$

Für $k = 4$ setzen wir fort mit

$$\begin{aligned} \hat{r}_4 &= \hat{r}_2 \bmod \hat{r}_3 = 5 \bmod 3 = 2, & \hat{q}_4 &= \hat{r}_2 \operatorname{div} \hat{r}_3 = 5 \operatorname{div} 3 = 1, \\ \hat{x}_4 &= \hat{x}_2 - \hat{q}_4\hat{x}_3 = 1 + 1 \cdot 5 = 6, & \hat{y}_4 &= \hat{y}_2 - \hat{q}_4\hat{y}_3 = -1 - 1 \cdot 6 = -7. \end{aligned}$$

Für $k = 5$ setzen wir fort mit

$$\begin{aligned} \hat{r}_5 &= \hat{r}_3 \bmod \hat{r}_4 = 3 \bmod 2 = 1, & \hat{q}_5 &= \hat{r}_3 \operatorname{div} \hat{r}_4 = 3 \operatorname{div} 2 = 1, \\ \hat{x}_5 &= \hat{x}_3 - \hat{q}_5\hat{x}_4 = -5 - 1 \cdot 6 = -11, & \hat{y}_5 &= \hat{y}_3 - \hat{q}_5\hat{y}_4 = 6 + 1 \cdot 7 = 13. \end{aligned}$$

Schließlich erreichen wir für $k = 6$ das Abbruchkriterium $\hat{r}_6 = \hat{r}_4 \bmod \hat{r}_5 = 2 \bmod 1 = 0$. Damit löst $(\hat{x}, \hat{y}) = (\hat{x}_5, \hat{y}_5) = (-11, 13) \in \mathbb{Z}^2$ die Gleichung $33\hat{x} + 28\hat{y} = 1$, und wir erhalten das multiplikative Inverse $28^{-1} = 13 \bmod 33 = 13$ in $\mathbb{Z}_{33}$.

Die Lösung der Gleichung $28x \equiv 119 \,(\mathrm{mod}\, 33)$ ist dann $x \equiv 28^{-1} \cdot 119 \equiv 13 \cdot 119 \,(\mathrm{mod}\, 33)$. Aus $119 \equiv 20 \,(\mathrm{mod}\, 33)$ und $13 \cdot 20 = 260 \equiv 29 \,(\mathrm{mod}\, 33)$ folgt somit $x = 29$ in $\mathbb{Z}_{33}$.

b) Da 11 und 13 Primzahlen sind und $\mathrm{ggT}(3, 11) = 1$ sowie $\mathrm{ggT}(2, 13) = 1$ gilt, liefert der kleine Satz von Fermat die Kongruenzen $3^{11-1}(\mathrm{mod}\ 11) = 1$ und $2^{13-1}(\mathrm{mod}\ 13) = 1$. □

PRÄSENZAUFGABE.

a) Zeigen Sie, dass $(\mathbb{Z}_7, +, \cdot)$ ein Körper ist, wenn Addition $+$ bzw. Multiplikation $\cdot$ wie üblich erklärt sind:

$$(a, b) \mapsto (a + b) \bmod 7 \quad \text{bzw.} \quad (a, b) \mapsto (a \cdot b) \bmod 7 \quad \text{für } a,\, b \in \mathbb{Z}_7.$$

b) Jeder unendlichen Folge $(p_0, p_1, \ldots, p_k, \ldots)$, deren Glieder $p_k \in \mathbb{Z}_7$ die Eigenschaft haben, dass $p_k \neq 0 \in \mathbb{Z}_7$ nur für endlich viele $k \in \mathbb{N}_0$ gilt, soll ein

$$\textit{Polynom } p = \sum_{k \in \mathbb{N}_0} p_k x^k \ \textit{ über } \mathbb{Z}_7$$

mit den Koeffizienten p_k als endliche Summe zugeordnet werden, wobei zu beachten ist, dass x *keine* Variable ist! Die Zahl

$$n_p = \max\{k \in \mathbb{N}_0 : p_k \neq 0\}$$

heißt *Grad* von $p \in \mathbb{Z}_7[x]$. Die Koeffizienten $p_k \in \mathbb{Z}_7$ von p mit größeren Indizes verschwinden also: Für alle $k > n_p$ gilt $p_k = 0 \in \mathbb{Z}_7$. Ist $\mathbb{Z}_7[x]$ die Menge aller Polynome p über $\mathbb{Z}_7$, so werden Addition und Multiplikation in $\mathbb{Z}_7[x]$ durch

$$p + q = \sum_{k \in \mathbb{N}_0} (p_k + q_k)\, x^k \quad \text{sowie} \quad p \cdot q = \sum_{k \in \mathbb{N}_0} \sum_{j \in \mathbb{N}_0} p_k \cdot q_j \, x^{k+j}$$

definiert. Sind zwei Polynome p und m in $\mathbb{Z}_7[x]$ durch $p = 4x^3 + 4x^2 + 2x + 2$ sowie $m = x^2 + 3$ gegeben, so berechne man die Restklasse $r = p \bmod m$ in $\mathbb{Z}_7[x]$!

Lösung. a) $(\mathbb{Z}_7, +)$ ist laut Vorlesung eine kommutative Gruppe mit neutralem Element $0 \in \mathbb{Z}_7$. Es wird gezeigt, dass $(\mathbb{Z}_7 \setminus \{0\}, \cdot)$ eine kommutative Gruppe mit neutralem Element $1 \in \mathbb{Z}_7$ ist:

Das Assoziativgesetz $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ folgt aus den Regeln der Modulorechnung:

$$\begin{aligned}(a \cdot b) \cdot c \bmod 7 &= (a \cdot b \bmod 7) \cdot (c \bmod 7) \\ &= (a \bmod 7) \cdot (b \bmod 7) \cdot (c \bmod 7) \\ &= (a \bmod 7) \cdot (b \cdot c \bmod 7) = a \cdot (b \cdot c) \bmod 7.\end{aligned}$$

Das Kommutativgesetz $a \cdot b = b \cdot a$ folgt aus der Symmetrie des Diagramms

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

und die Existenz eines Einselements $1 \in \mathbb{Z}_7$ ist offensichtlich. Außerdem kann man erkennen, dass alle Elemente aus $\mathbb{Z}_7 \setminus \{0\}$ ein multiplikatives Inverses besitzen.

Das Distributivgesetz $a \cdot (b + c) = a \cdot b + a \cdot c$ ergibt sich ebenfalls aus den Regeln der Modulorechnung:

$$\begin{aligned} a \cdot (b+c) \bmod 7 &= (a \bmod 7) \cdot ((b+c) \bmod 7) \\ &= (a \bmod 7) \cdot (b \bmod 7) + (a \bmod 7) \cdot (c \bmod 7) \\ &= (a \cdot b \bmod 7) + (a \cdot c \bmod 7) = (a \cdot b + a \cdot c) \bmod 7. \end{aligned}$$

Damit ist gezeigt, dass $\mathbb{Z}_7$ ein Körper ist.

b) Zunächst gilt

$$p = 4x^3 + 4x^2 + 2x + 2 = 4x \cdot (x^2 + 3) + 4x^2 - 10x + 2 = 4x \cdot m + r_1 \in \mathbb{Z}_7[x]$$

mit einem Restpolynom $r_1 = 4x^2 - 10x + 2 \in \mathbb{Z}_7[x]$, das einen kleineren Grad als p hat. Aus diesem Restpolynom r_1 kann man noch ein Vielfaches von m herauslösen: Es gilt

$$r_1 = 4x^2 - 10x + 2 = 4 \cdot (x^2 + 3) - 10x - 10 = 4 \cdot m + r_2 \in \mathbb{Z}_7[x]$$

mit dem Restpolynom $r_2 = -10x - 10 \in \mathbb{Z}_7[x]$, dessen Grad kleiner als der Grad von m ist. Somit ergibt sich

$$p = (4x + 4) \cdot m - 10x - 10 \in \mathbb{Z}_7[x],$$

und wegen $-10 \equiv 4 \,(\mathrm{mod}\ 7)$ erhält man schließlich $p \equiv 4x + 4 \,(\mathrm{mod}\ m)$ in $\mathbb{Z}_7[x]$. □