Mathematisches Institut
der Universität München
Pascal Reisert

Wintersemester 2015/2016
Übungsblatt 1
21. Oktober 2015

Übungen zur Algorithmischen Zahlentheorie
Lösung

Aufgabe 2

Wir identifizieren $\mathfrak{B}$ mit $\{\texttt{A}, \ldots, \texttt{Z}\}$, sodass sich der Code wie folgt liest

```
ATSUOBARDUOPBORTOMUSBBJSQ
HXTSKUSLABHBAOMJHLATSDJFS
LAPKSORATSJDLQHLCUSLWTHQT
HLFOMFSBDQHXTSKQOLBHBAHLC
ORBAHQIUSLSDQTXOBSKSXKSBS
LAHLCDJHBAHLQAMSAASK.
```

Wir bestimmen zunächst die Häufigkeit der verschiedenen Buchstaben und erhalten:

Buchstabe	Anzahl	Buchstabe	Anzahl	Buchstabe	Anzahl
S	20	K	6	I	1
A	14	J	5	W	1
B	13	X	4	E	0
L	13	M	4	G	0
H	13	R	4	N	0
O	10	C	3	V	0
T	9	F	3	Y	0
Q	8	P	2	Z	0
U	6	D	6		

Als nächstes bestimmen wir alle Abfolgen von mehr als drei Buchstaben die sich wiederholen:

- 2fach QHXTSK,
- 2fach BHBAHL + 1fach BHBA+ 1fach BAH + 1fach AHL,
- 3fach ATS,
- 3fach USL,
- 3fach SLA,
- 3fach HLC.

```
ATSUOBARDUOPBORTOMUSBBJSQ
HXTSKUSLABHBAOMJHLATSDJFS
LAPKSORATSJDLQHLCUSLWTHQT
HLFOMFSBDQHXTSKQOLBHBAHLC
ORBAHQIUSLSDQTXOBSKSXKSBS
```

LAHLCDJHBAHLQAMSAASK.

Wir erhoffen uns, dass zumindest eine dieser Kombination den englischen Artikel the darstellt. Überprüfen wir für welche der Kombinationen auch holmes möglich ist. Für die Kombinationen H***X, X***T , T***S, S***K, H***B, B***A, A***H, H***L, S***L, L***A, , L***C ergeben sich die folgenden vorkommenden verschlüsselten Worte für holmes

- TOMUSB, TSKUSL, TXOBSK,
- SKSXKS, SAASK.,
- AOMJHL,
- SKUSLA, SKQOLB, SLAHLC,
- HQTHLF, HBAHLC, HBAHLQ,
- LBHBAH, LQHLCU , LAHLCD.

Davon haben nur TOMUSB, TXOBSK, AOMJHL, SKQOLB die richtige Form. Die zugehörigen Triagramme sind XTS, ATS, BAH, USL, wovon XTS und BAH in längeren Kombinationen auftreten. Da wir das Wortende jedoch nicht kennen könnten sie natürlich auch the darstellen. Von den Triagrammen ATS und USL ist ATS wahrscheinlicher, da der Buchstabe A mit einer Häufigkeit von 9,66% auftritt, wohingegen U nur 4,14 % der Buchstaben ausmacht. Die für den Buchstaben t erwartete Häufigkeit ist jedoch 9,25 %. Man beachte B hat eine Häufigkeit von 8,97 % und X nur eine Häufigkeit von 2,76 %.
Um eine möglichst gute Wahl treffen zu können vergleichen wir weitere Buchstaben von TOMUSB, TXOBSK und AOMJHL auf Häufigkeit.

Buchstabe	TOMUSB	TXOBSK	AOMJHL
e (12,75 %)	S (13,79 %)	S (13,79 %)	H (8,97 %)
o (7,5 %)	O (6,90 %)	X (2,76 %)	O (6,90 %)
s (6,0 %)	B (8,97 %)	K (4,14 %)	L (8,97 %).

Wir erhalten die Abweichungen von (e,o,s) als

TOMUSB	$\sqrt{0,5 \cdot ((12,75-13,79)^2+(7,5-6,9)^2+(6,0-8,97)^2)} = 2,26$
TXOBSK	$\sqrt{0,5 \cdot ((12,75-13,79)^2+(7,5-2,76)^2+(6,0-4,14)^2)} = 3,67$
AOMJHL	$\sqrt{0,5 \cdot ((12,75-8,97)^2+(7,5-6,9)^2+(6,0-8,97)^2)} = 3,43.$

Nach diesen Beobachtungen vermuten wir, dass holmes gerade durch TOMUSB dargestellt wird und ATS folglich the ist. Unser Alphabeth nimmt damit die folgende Form an

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ts          l o   ehm
```

Setzen wir alle bereits bekannten Buchstaben ein, dann ergibt sich

```
ATSUOBARDUOPBORTOMUSBBJSQ
themost  mo so holmess e
HXTSKUSLABHBAOMJHLATSDJFS
  he me ts stol   the   e
```

```
LAPKSORATSJDLQHLCUSLWTHQT
 t  eo the       me  h  h
HLFOMFSBDQHXTSKQOLBHBAHLC
   ol es    he  o s st
ORBAHQIUSLSDQTXOBSKSXKSBS
o st   me e  h ose e  ese
LAHLCDJHBAHLQAMSAASK.
 t      st   tlette .
```

Betrachten wir unseren Lückentext genau, so lässt sich am Ende des Textes das Wort `letter` erkennen. Wir erhalten

```
ATSUOBARDUOPBORTOMUSBBJSQ
themost  mo so holmess e
HXTSKUSLABHBAOMJHLATSDJFS
  herme ts stol   the   e
LAPKSORATSJDLQHLCUSLWTHQT
 t reo the       me  h  h
HLFOMFSBDQHXTSKQOLBHBAHLC
   ol es    her o s st
ORBAHQIUSLSDQTXOBSKSXKSBS
o st   me e  h osere rese
LAHLCDJHBAHLQAMSAASK.
 t      st   tletter.
```

Wir betrachten wiederum die Häufigkeiten der verbleibenden Buchstaben. In unserem Text treten `L, H` häufig auf, in der englischen Sprache sind die noch nicht verwendeten häufigsten Buchstaben `n,i,a`. Die Kombination `USLS=me*e` in der fünften Zeile unseres Textes lässt vermuten, dass `L` kein Vokal ist, also versuchen wir `L=n`.

```
ATSUOBARDUOPBORTOMUSBBJSQ
themost  mo so holmess e
HXTSKUSLABHBAOMJHLATSDJFS
  herments stol  nthe   e
LAPKSORATSJDLQHLCUSLWTHQT
nt reo the  n  n men h  h
HLFOMFSBDQHXTSKQOLBHBAHLC
 n ol es    her ons st n
ORBAHQIUSLSDQTXOBSKSXKSBS
o st   mene  h osere rese
LAHLCDJHBAHLQAMSAASK.
nt n    st n tletter.
```

Für `H` betrachten wir die beiden Möglichkeiten

```
H=a                          H=i

ATSUOBARDUOPBORTOMUSBBJSQ    ATSUOBARDUOPBORTOMUSBBJSQ
themost  mo so holmess e     themost  mo so holmess e
HXTSKUSLABHBAOMJHLATSDJFS    HXTSKUSLABHBAOMJHLATSDJFS
```

```
a hermentsastol anthe   e
LAPKSORATSJDLQHLCUSLWTHQT
nt reo the  n an men ha h
HLFOMFSBDQHXTSKQOLBHBAHLC
an ol es  a her onsastan
ORBAHQIUSLSDQTXOBSKSXKSBS
o sta  mene  h osere rese
LAHLCDJHBAHLQAMSAASK.
ntan   astan tletter.
```

```
i hermentsistol inthe   e
LAPKSORATSJDLQHLCUSLWTHQT
nt reo the  n in men hi h
HLFOMFSBDQHXTSKQOLBHBAHLC
in ol es  i her onsistin
ORBAHQIUSLSDQTXOBSKSXKSBS
o sti  mene  h osere rese
LAHLCDJHBAHLQAMSAASK.
ntin   istin tletter.
```

Wir erkennen auf der rechten Seite das Wort `consisting`. Wir versuchen deshalb mit `H=i` weiter aufzulösen.

```
ATSUOBARDUOPBORTOMUSBBJSQ
themost  mo so holmess ec
HXTSKUSLABHBAOMJHLATSDJFS
i hermentsistol inthe   e
LAPKSORATSJDLQHLCUSLWTHQT
nt reo the  ncingmen hich
HLFOMFSBDQHXTSKQOLBHBAHLC
in ol es ci herconsisting
ORBAHQIUSLSDQTXOBSKSXKSBS
o stic mene ch osere rese
LAHLCDJHBAHLQAMSAASK.
nting  istinctletter.
```

In der zweiten Zeile erkennen wir das Satzfragment `is told in the`. In der vierten Zeile könnte es `consisting of` heißen.

```
ATSUOBARDUOPBORTOMUSBBJSQ
themostf mo sofholmessdec
HXTSKUSLABHBAOMJHLATSDJFS
i hermentsistoldinthe d e
LAPKSORATSJDLQHLCUSLWTHQT
nt reofthed ncingmen hich
HLFOMFSBDQHXTSKQOLBHBAHLC
in ol es ci herconsisting
ORBAHQIUSLSDQTXOBSKSXKSBS
ofstic mene ch osere rese
LAHLCDJHBAHLQAMSAASK.
nting distinctletter.
```

Sowohl `decipherment` in Zeile 1f sowie auch `cipher` in Zeile vier, deuten auf `X=p` hin.

```
ATSUOBARDUOPBORTOMUSBBJSQ
themostf mo sofholmessdec
HXTSKUSLABHBAOMJHLATSDJFS
iphermentsistoldinthe d e
LAPKSORATSJDLQHLCUSLWTHQT
nt reofthed ncingmen hich
```

```
HLFOMFSBDQHXTSKQOLBHBAHLC
in ol es cipherconsisting
ORBAHQIUSLSDQTXOBSKSXKSBS
ofstic mene chposereprese
LAHLCDJHBAHLQAMSAASK.
nting distinctletter.
```

Wir schließen weiter mit `of the d*ncing men` auf `D=a`

```
ATSUOBARDUOPBORTOMUSBBJSQ
themostfamo sofholmessdec
HXTSKUSLABHBAOMJHLATSDJFS
iphermentsistoldinthead e
LAPKSORATSJDLQHLCUSLWTHQT
nt reofthedancingmen hich
HLFOMFSBDQHXTSKQOLBHBAHLC
in ol esacipherconsisting
ORBAHQIUSLSDQTXOBSKSXKSBS
ofstic meneachposereprese
LAHLCDJHBAHLQAMSAASK.
ntingadistinctletter.
```

Schließlich ergeben sich die verbleibenden Buchstaben leicht zu:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
tsga v ikdrnl oucfehm wp
```

```
ATSUOBARDUOPBORTOMUSBBJSQ
themostfamousofholmessdec
HXTSKUSLABHBAOMJHLATSDJFS
iphermentsistoldintheadve
LAPKSORATSJDLQHLCUSLWTHQT
ntureofthedancingmenwhich
HLFOMFSBDQHXTSKQOLBHBAHLC
involvesacipherconsisting
ORBAHQIUSLSDQTXOBSKSXKSBS
ofstickmeneachposereprese
LAHLCDJHBAHLQAMSAASK.
ntingadistinctletter.
```

The most famous of Holmes's decipherments is told in "the adventure of the dancing men", which involves a cipher consisting of stickmen, each pose representing a distinct letter.

Aufgabe 3

a) Die Komposition ist wohldefiniert auf $\mathrm{Aff}(2, \mathbb{Z}_{26})$, da für alle $\varphi, \psi \in \mathrm{Aff}(2, \mathbb{Z}_{26})$ gilt:

$$\begin{aligned} &\varphi(x) = Ax + t, \psi(x) = Bx + s \text{ für } A, B \in \mathrm{Gl}(2, \mathbb{Z}_{26}),\ s, t, \in \mathbb{Z}_{26}^2 \\ &\Rightarrow \varphi(\psi(x)) = ABx + (As + t) \in \mathrm{Aff}(2, \mathbb{Z}_{26}). \end{aligned}$$

Das neutrale Element ist die Identität, das Inverse Element zu φ ist $x \mapsto A^{-1}x - A^{-1}t$. Damit ist $\mathrm{Aff}(2, \mathbb{Z}_{26})$ eine Gruppe.

Mit dem chinesischen Restsatz wissen wir, dass $\mathbb{Z}_{26} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{13}$. Wir bestimmen die Anzahl der invertierbaren Elemente in $\mathrm{Gl}(k)$ für einen beliebeigen endlichen Körper k mit p Elementen. Eine Matrix $A = (a_1, a_2) \in \mathrm{Gl}(k)$ ist genau dann invertierbar, wenn ihre Spalten a_1 und a_2 linear unabhängig sind. Für a_1 haben wir die Wahl $p^2 - 1$ (zwei Einträge ohne dem Nullvektor). Weiter soll gelten $a_2 \neq xa_1,\ x \in k$, also haben wir $p^2 - p$ Möglichkeiten. Insgesamt hat $\mathrm{Gl}(k)$ damit $(p^2-1)(p^2-p)$ Elemente. Ein Automorphimus von $\mathbb{Z}_2 \times \mathbb{Z}_{13}$ hat jetzt die Form

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

mit $\alpha \in \mathrm{End}(2, \mathbb{Z}_2),\ \delta \in \mathrm{End}(2, \mathbb{Z}_{13})$ und $\beta \in \mathrm{Hom}_2(\mathbb{Z}_{13}, \mathbb{Z}_2), \gamma \in \mathrm{Hom}_2(\mathbb{Z}_2, \mathbb{Z}_{13})$. Aufgrund der verschiedenen Charakteristiken gilt $\beta, \gamma = 0$ also $\alpha \in \mathrm{Gl}(2, \mathbb{Z}_2),\ \delta \in \mathrm{Gl}(2, \mathbb{Z}_{13})$ und wir erhalten die Anzahl der Element von $\mathrm{Gl}(2, \mathbb{Z}_{26})$ zu

$$(2^2 - 1)(2^2 - 2)(13^2 - 1)(13^2 - 13) = 157248.$$

Die Gruppe $\mathrm{Aff}(2, \mathbb{Z}_{26})$ hat dann

$$26^2 \cdot 157248 = 4088448$$

Elemente. Hierbei haben wir verwendet, dass aus $Ax + t = Bx + s, \forall x \in \mathbb{Z}_{26}^2$ bereits für $x = 0 \Rightarrow s = t$ und somit $Ax = Bx, \forall x \in \mathbb{Z}_{26}^2$ folgt. Man kann die Anzahl der Elemente von $\mathrm{Gl}(2, \mathbb{Z}_{26})$ auch direkt bestimmen: Eine Matrix A ist genau dann invertierbar, wenn ihre Determinante invertierbar, d.h. eine Einheit, ist. $\mathbb{Z}_{26}$ besitzt die 12 Einheiten

$$\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$$

Sei $\det(A) = ad - bc$ die Determinante von $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. $\det(A) = u \in \mathbb{Z}_{26}^*$ kann nur gelten, wenn genau einer der Summanden ungerade ist. Wir bestimmen die Häufigkeiten mit der eine Zahl $m \in \mathbb{Z}_{26}$ als Produkt zweier Zahlen auftritt:

- 0 ergibt sich 75fach: $0 \cdot d$ für d beliebig, $a \cdot 0$ für $a \neq 0$ und $13 \cdot c$, $c \neq 0$ gerade, sowie $b \cdot 13$ mit $b \neq 0$ gerade.
- 13 erhält man auf 25 verschiedenen Weisen: $13 \cdot d$ für d ungerade und $a \cdot 13$ für $a \neq 13$ und ungerade.
- Jede gerade Zahlen ungleich 0 tritt 36fach auf, jede ungerade Zahl ungleich 13 genau 12fach.

Um den letzten Punkt zu verstehen beachte man, dass der Gruppenautomorphismus $\mathbb{Z}_{26} \to \mathbb{Z}_{26}, x \mapsto 7 \cdot x$ genau die Mengen $\mathbb{Z}_{26}^*, (2) \setminus \{0\}, \{0\}, \{13\}$ erhält. Somit gilt $(7^k a, d) = (7^k a', d')$ für zwei Lösung von $7^k ad = 7^k m = 7^k a' d'$ genau dann wenn $d = d', 7^k a = 7^k a' \Leftrightarrow a = a', d = d'$. Es folgt

$$\frac{13 \cdot 39 - 75}{12} = 36, \quad \frac{13 \cdot 13 - 25}{12} = 12.$$

wobei wir die Anzahl der Lösungen (a, d) von $a \cdot d = m$ gerade und ungleich 0 durch die Anzahl der Elemente von $(2) \setminus \{0\}$ geteilt haben. Dies ist möglich da wir wissen, dass es

für jedes $m \in (2) \setminus \{0\}$ gleich viele Lösungen von $a \cdot d = m$ gibt. Analog verfahren wir mit $m \in \mathbb{Z}_{26}^*$.
Wir bekommen einen Faktor 2 für die Wahl zwischen ad oder bc ungerade. Es gibt 12^2 Paare ungerader Zahlen. Jedoch sind nur $11 \cdot 36 + 75$ der Summen $\neq 13$. Also haben wir bereits

$$2 \cdot 12^2 \cdot (11 \cdot 36 + 75)$$

Lösungen gefunden. Wie wir gesehen haben gibt es weitere 25 Möglichkeiten eine ungerade Zahl mit Teiler 13 zu kombinieren. Der zugehörige gerade Summand darf nicht 0 werden, also weitere $12 \cdot 36$ Möglichkeiten. Insgesamt also wie erwartet

$$2 \cdot 12^2 \cdot (11 \cdot 36 + 75) + 2 \cdot 25 \cdot 12 \cdot 36 = 157248.$$

b) Man identifiziere

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Damit müssen wir A, t wie zuvor finden mit

$$A \cdot \begin{pmatrix} 1 & 2 & 18 \\ 12 & 5 & 20 \end{pmatrix} + (t,t,t) = \begin{pmatrix} 10 & 19 & 16 \\ 15 & 5 & 8 \end{pmatrix}$$

Subtrahiert man die zweite resp. dritte Spalte von der ersten so erhält ma

$$A \cdot \begin{pmatrix} -1 & 9 \\ 7 & -8 \end{pmatrix} = \begin{pmatrix} -9 & -6 \\ 10 & 7 \end{pmatrix}$$

Wir erkennen $\det \begin{pmatrix} -1 & 9 \\ 7 & -8 \end{pmatrix} = -3 \in \mathbb{Z}_{26}^*$ und

$$\begin{pmatrix} -1 & 9 \\ 7 & -8 \end{pmatrix}^{-1} = 17 \cdot \begin{pmatrix} -8 & -9 \\ -7 & -1 \end{pmatrix} = \begin{pmatrix} -6 & 3 \\ 11 & 9 \end{pmatrix}.$$

Schließlich ist

$$A = \begin{pmatrix} -9 & -6 \\ 10 & 7 \end{pmatrix} \begin{pmatrix} -6 & 3 \\ 11 & 9 \end{pmatrix} = \begin{pmatrix} 14 & -3 \\ 17 & 15 \end{pmatrix}.$$

Es folgt

$$A \begin{pmatrix} 1 & 2 & 18 \\ 12 & 5 & 20 \end{pmatrix} - \begin{pmatrix} 10 & 19 & 16 \\ 15 & 5 & 8 \end{pmatrix} = \begin{pmatrix} 4 & 13 & 10 \\ -11 & 5 & 8 \end{pmatrix} - \begin{pmatrix} 10 & 19 & 16 \\ 15 & 5 & 8 \end{pmatrix} = \begin{pmatrix} -6 & -6 & -6 \\ 0 & 0 & 0 \end{pmatrix}.$$

Damit haben wir eine eindeutige affine Abbildung gefunden, die `ALBERT` in `JOSEPH` überführt.
Für den Code `JOHANN` verfahren wir analog:

$$A \cdot \begin{pmatrix} 1 & 2 & 18 \\ 12 & 5 & 20 \end{pmatrix} + (t,t,t) = \begin{pmatrix} 10 & 8 & 14 \\ 15 & 1 & 14 \end{pmatrix}$$

und

$$A = \begin{pmatrix} 2 & -4 \\ 14 & 1 \end{pmatrix} \begin{pmatrix} -6 & 3 \\ 11 & 9 \end{pmatrix} = \begin{pmatrix} -4 & -4 \\ 5 & -1 \end{pmatrix}$$

Es folgt

$$A \begin{pmatrix} 1 & 2 & 18 \\ 12 & 5 & 20 \end{pmatrix} - \begin{pmatrix} 10 & 8 & 14 \\ 15 & 1 & 14 \end{pmatrix} = \begin{pmatrix} 0 & -2 & 4 \\ -7 & 5 & -8 \end{pmatrix} - \begin{pmatrix} 10 & 8 & 14 \\ 15 & 1 & 14 \end{pmatrix} = \begin{pmatrix} -10 & -10 & -10 \\ 4 & 4 & 4 \end{pmatrix}.$$

Damit haben wir eine affine Abbildung gefunden.