5.13 Bem: Wir wollen die geheimen Zahlen verstehen, die man mittels der Anweisung in 5.1 produzieren kann, ausgehend von einer Zahl a mit n Ziffern, also von $a = a_1 \cdots a_n$, mit $a_1 > a_n$. Die Subtraktion $a_1 \cdots a_n - a_n \cdots a_1$ haben wir bereits analysiert. Jetzt kommt im zweiten Schritt noch eine Addition zweier Zahlen, in unserem Fall von $b_1 \cdots b_n + b_n \cdots b_1$. Hierbei gibt es wieder einen Übertragsvektor $v_1 \cdots v_n (v_{n+1})$. Wir definieren diesen, sowie die Ziffern der geheimen Zahl durch:

$$
\begin{array}{lcccccccl}
(+) & & b_1 & \cdots & b_k & \cdots & b_{n-1} & b_n & \\
 & + & b_n & \cdots & b_{n-k+1} & \cdots & b_2 & b_1 & \\
 & & v_1 & v_2 \cdots & v_{k+1} & \cdots & v_n & v_{n+1} & \text{Übertragsvektor} \\
\hline
 & & v_1 & c_1 \cdots & c_k & \cdots & c_{n-1} & c_n & \text{geheime Zahl}
\end{array}
$$

In unserem Fall ist $b_1 \cdots b_n = a_1 \cdots a_n - a_n \cdots a_1$.
Nach 5.7(c) ist also

$$b_k = t_k B + a_k - (a_{n-k+1} + t_{k+1})$$

Beim Addieren in (+) bilden wir dann die folgenden Teilsummen:

$$
\begin{aligned}
R_k := b_k + b_{n-k+1} &= \text{Summe zu Ziffer } c_k \text{, ohne Übertrag} \\
&\overset{5.7(c)}{=} t_k B + a_k - (a_{n-k+1} + t_{k+1}) + t_{n-k+1} B + a_{n-k+1} - (a_k + t_{n-k+2}) \\
&= (t_k + t_{n-k+1}) B - (t_{k+1} + t_{n-k+2}) \quad , \quad 1 \le k \le n .
\end{aligned}
$$

Diese Teilsummen $R_1, \ldots, R_n$ hängen also nicht mehr von den Ziffern a_k der Zahl a ab, sondern nur noch vom Übertragungsvektor. Es gilt:

$$R_{n-k+1} = \underline{\qquad\qquad\qquad\qquad} = R_k, \quad 1 \le k \le n.$$

Außerdem gilt, daß $R_k \in \{0, B-2, B-1, B, 2B-2\}$ ist, für $1 \leq k \leq n$, denn:

Wir zeigen:

5.14 <u>Prop</u>: Mit der Notation aus 5.13 gilt:

(a) Die Abbildung $(t_1 \cdots t_n) \longmapsto (R_1, \dots, R_n)$ ist injektiv.

(b) Die Abbildung $(R_1, \dots, R_n) \longmapsto v_1 c_1 \cdots c_n$ ist injektiv.

Mit diesem Resultat folgt dann:

5.15 <u>Thm</u> (Anzahl geheimer Zahlen)

Sei $n \in \mathbb{N}^{\geq 2}$ mit $n = 2r$ oder $n = 2r+1$ für $r \in \mathbb{N}$.
Es gibt zu fest gewähltem n genau F_{2r} viele verschiedene geheime Zahlen wie in 5.1 konstruiert.

<u>Beweis</u>: Sei $Z_n := \{a_1 \cdots a_n \mid a_1 > a_n\}$

$T_n := \{$ Übertragsvektor $t_1 \cdots t_n$ zu $a \in Z_n \}$

$= \{ \tau_n(a) \mid a \in Z_n \}$

$R^n := \{ (R_1, \dots, R_n) \mid R_i$ gehören zu $t \in T_n \}$

$G_n := \{$geheime Zahlen zu $a \in Z_n \}$

Dann folgt aus 5.14 und 5.12(b):

$$|G_n| \overset{5.14(b)}{=} |R^n| \overset{5.14(a)}{=} |T_n| \overset{5.12(b)}{=} F_{2n}.$$

5.16 <u>Bsp</u>: $n = 3$: nach 5.1 + 5.2 gilt $|G_3| =$ _____

$n = 4$: nach 5.5 ist $|G_4| =$ _____

$n = 5$: Nach 5.15 ist $|G_5| =$ _____

$n = 6$: Nach 5.15 ist $|G_6| =$ _____

5.17 <u>Beweis zu Prop 5.14 (a)</u>:

(a) Gegeben sind $R_1, \dots, R_n$. Wir zeigen, daß $\tau_n(a) = t_1 \dots t_n$ eindeutig durch $R_1, \dots, R_n$ bestimmt ist. Dies zeigt die Injektivität der Abbildung $t_1 \dots t_n \longrightarrow (R_1, \dots, R_n)$. Wir beweisen dies mittels Induktion nach k, indem wir rekursiv von Außen nach Innen arbeiten.

Induktionsanfang: $k = 1$.
Nach Lemma 5.7 (a) ist $t_1 = 0$ und $t_n = 1$, für jeden Übertragungsvektor $\tau_n(a) \in T_n$. Nach 5.13 gilt für $k=1$:

$$R_1 = (\underset{0}{t_1} + \underset{1}{t_n})\, B - (t_2 + \underset{0}{t_{n+1}}) = B - t_2$$

$\Rightarrow t_2 = B - R_1$ ist eindeutig durch $R_1, \dots, R_n$ bestimmt. Wir kennen jetzt t_1, t_2 und t_n. Im nächsten Schritt konstruiert man nun t_3 und t_{n-1}.

(b) Sei $k \geq 2$ und seien $t_1, \dots, t_k$ und $t_{n-k+2}, \dots, t_n$ bekannt. Wir konstruieren t_{n-k+1} und t_{k+1} aus der Gleichung

$$R_k \overset{5.13}{=} (t_k + t_{n-k+1})\, B - (t_{k+1} + t_{n-k+2}) \quad (\Delta)$$

Das Problem ist also, daß wir eine Gleichung haben, und aus dieser zwei Variablen eindeutig bestimmen wollen. Allerdings haben wir Zusatzbedingungen

- $R_k \in \{0, B-2, B-1, B, 2B-2\}$ nach 5.13
- alle t_i's sind aus $\{0,1\}$.

Die Anzahl der Gleichungen, die hier gelöst werden müssen, ist damit klein. Wir unterscheiden je nach den bekannten Werten von t_k und t_{n-k+2} vier Fälle:

1. Fall: Sei $t_k = 0 = t_{n-k+2}$. Dann gilt:

	R_k	0	$B-2$	$B-1$	B	$2B-2$
gesuchte Werte	t_{n-k+1}	0	$\lightning$	1	0	$\lightning$
	t_{k+1}	0		1	1	

und damit sind in diesem Fall die Überträge t_{k+1} und t_{n-k+1} eindeutig bestimmt durch R_k.

- Beispielsweise können die Fälle $R_k = B-2$ oder $R_k = 2B-2$ nicht vorkommen, denn Gleichung (Δ) muß nach Konstruktion eine Lösung haben.
- Der Fall $R_k = B-1 \overset{(\Delta)}{=} t_{n-k+1} B - t_{k+1}$ liefert aufgrund der Eindeutigkeit der B-adischen Zahlendarstellung (siehe 4.3): $t_{n-k+1} = 1 = t_{k+1}$.

Etc. Analog sind die anderen Fälle zu lösen:

2. Fall: Sei $t_k = 1$, $t_{n-k+2} = 0$. Dann gilt:

R_k	0	$B-2$	$B-1$	B	$2B-2$
t_{n-k+1}	$\lightning$	$\lightning$	0	0	$\lightning$
t_{k+1}			1	0	

3. Fall: Sei $t_k = 0$, $t_{n-k+2} = 1$. Dann gilt:

R_k	0	$B-2$	$B-1$	B	$2B-2$
t_{n-k+1}					
t_{k+1}					

4. Fall: Sei $t_k = 1 = t_{n-k+2}$. Dann gilt:

R_k	0	$B-2$	$B-1$	B	$2B-2$
t_{n-k+1}					
t_{k+1}					

Induktiv folgt: $\tau_n(a) = t_1 \cdots t_n$ ist eindeutig durch $R_1, \dots, R_n$ bestimmbar; die Abb. $t_1 \cdots t_n \longmapsto (R_1, \dots, R_n)$ ist also injektiv.

5.18 <u>Beweis zu Prop 5.14 (b):</u>

Gegeben ist das geheime Wort $v_1 c_1 \cdots c_n$. Wir zeigen, die Summen $(R_1, \dots, R_n)$ sind hierdurch eindeutig bestimmt. Dies zeigt die Injektivität der Abbildung $(R_1, \dots, R_n) \mapsto v_1 c_1 \cdots c_n$. Wir beweisen dies mittels Induktion nach k, indem wir rekursiv von Außen nach Innen arbeiten.

1. <u>Schritt:</u>

Nach 5.13 ist $R_n = (\overset{1}{\overset{\shortparallel}{t_n}} + \overset{0}{\overset{\shortparallel}{t_1}})\, B - (\overset{0}{\overset{\shortparallel}{t_{n+1}}} + t_2) \overset{5.7(a)}{=} B - t_2$

Hierbei sind jetzt R_n und t_2 Unbekannte. Wir wissen aber, daß $t_2 \in \{0,1\}$ ist und $R_n \in \{B, B-1\}$. Mit (+) folgt: entweder gilt

- $R_n = B$, $t_2 = 0$, $c_n = 0$, $v_n = 1$, oder
- $R_n = B-1$, $t_2 = 1$, $c_n = B-1$, $v_n = 0$.

Da wir c_n kennen, können wir R_n und t_2 eindeutig aus c_n konstruieren. Nach 5.13 gilt außerdem $R_n = R_1$. Dies ist der Induktionsanfang. Beachte v_1 ist bekannt, da Teil des geheimen Wortes.

2. <u>Schritt:</u> Seien $R_1 (\overset{5.13}{=} R_n)$, $R_2 (\overset{5.13}{=} R_{n-1}), \dots, R_k (\overset{5.13}{=} R_{n-k+1})$ bereits bestimmt, sowie die Elemente $v_1, \dots, v_k$ und $v_{n-k+1}, \dots, v_n$ bereits rekonstruiert und eindeutig durch das geheime Wort bestimmt.

Sei jetzt $k \geq 2$. Wir wollen $R_{k+1} (\overset{5.13}{=} R_{n-k})$ sowie v_{k+1} und v_{n-k} rekonstruieren. Schreibe B-adisch: $R_{k+1} =: (\alpha \alpha')_B$. Nach 5.13 hat R_{k+1} höchstens zwei Ziffern mit $\alpha \in \{0,1\}$ und $\alpha' \in \{0, B-1, B-2\}$.

3. <u>Schritt:</u> Wir bestimmen zunächst v_{k+1} aus Gleichung (+). Ist $R_k = (10)_B$ oder $R_k = (1\,B\text{-}2)_B$, so ist $c_k = \alpha'$ und $v_{k+1} = 0$. Nach 5.13 müssen wir nur noch $R_k \in \{0, 1, B-1\}$ betrachten. Ist hierbei $R_k = c_k$, so ist $v_{k+1} = 0$; ist $R_k \neq c_k$, so ist $v_{k+1} = 1$. Damit ist v_{k+1} eindeutig durch $v_1 c_1 \cdots c_n$ = geheime Wort bestimmt.

4. Schritt: Wir zeigen $R_{k+1} = (\alpha\alpha')_B$ ist eindeutig bestimmt.

Unsere Situation in (†) ist:

$$\begin{array}{lcccccc}
 & b_k & \left.\begin{matrix} b_{k+1} \\ b_{n-k} \end{matrix}\right\} = (\alpha\alpha')_B & & & \left.\begin{matrix} b_{n-k} \\ b_{k+1} \end{matrix}\right\} = (\alpha\alpha')_B & \\
 & b_{n-k+1} & & & & & \\
\text{bekannt nach 3. Schritt} \rightarrow & v_{k+1} & v_{k+2} & \cdots & v_{n-k} & v_{n-k+1} \leftarrow \text{bekannt nach Ind. Vor.} & \\
\hline
\cdots & c_k & c_{k+1} & \cdots & & c_{n-k} & \cdots
\end{array}$$

(a) Betrachte die Spalte der Ziffer c_{n-k}:

↳ Ist $v_{n-k+1} = 0$, so folgt $\alpha' =$ _____

↳ Ist $v_{n-k+1} = 1$ und $c_{n-k} = 0$, so folgt $\alpha' =$ _____

↳ Ist $v_{n-k+1} = 1$ und $c_{n-k} > 0$, so folgt $\alpha' =$ _____

Damit ist α' eindeutig bestimmbar.

(b) Betrachte die Spalte der Ziffer c_{k+1}:

↳ Ist $c_{k+1} = \alpha'$, so ist $\alpha =$ _____

↳ Ist $\alpha' \neq c_{k+1}$ und $c_{k+1} = 0$, so folgt $\alpha =$ _____

↳ Ist $\alpha' \neq c_{k+1}$ und $c_{k+1} > 0$, so folgt $\alpha =$ _____

Damit ist α eindeutig bestimmbar.

Insgesamt folgt in allen Fällen, daß die Teilsumme $R_{k+1} = (\alpha\alpha')_B$ durch das geheime Wort eindeutig bestimmt ist.

5. Schritt: Die Induktionsbehauptung (siehe Schritt 2) ist erst vollständig bewiesen, wenn wir zeigen, daß auch v_{n-k} eindeutig bestimmbar ist.