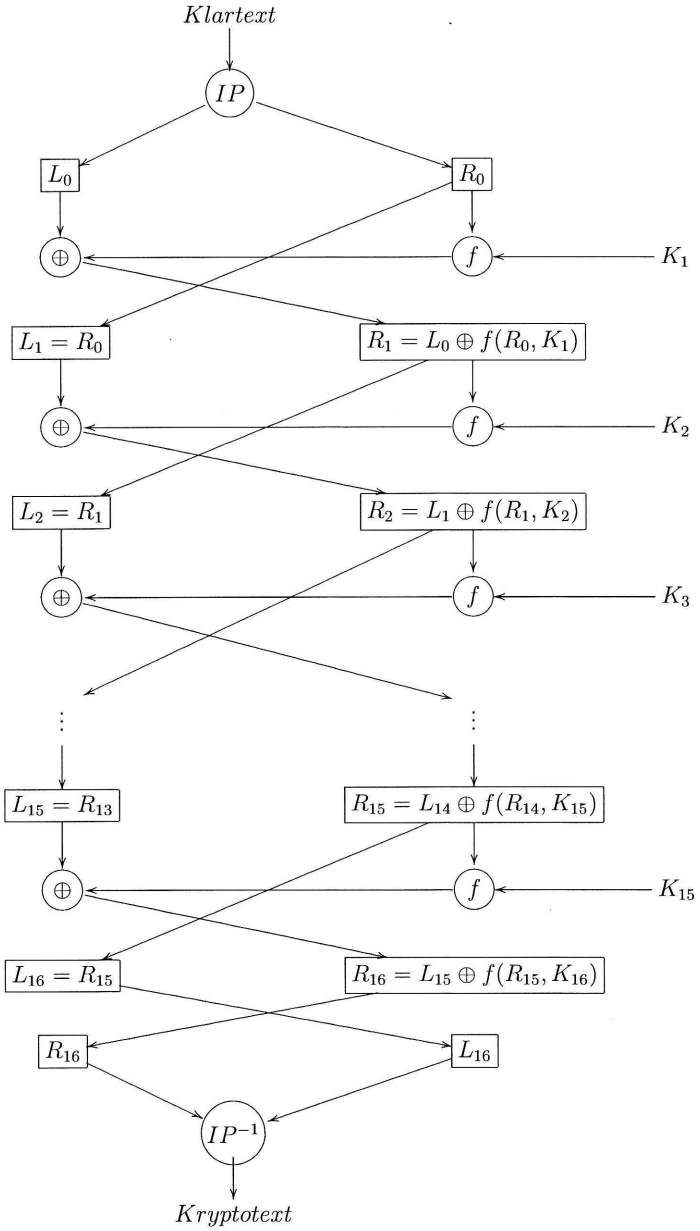
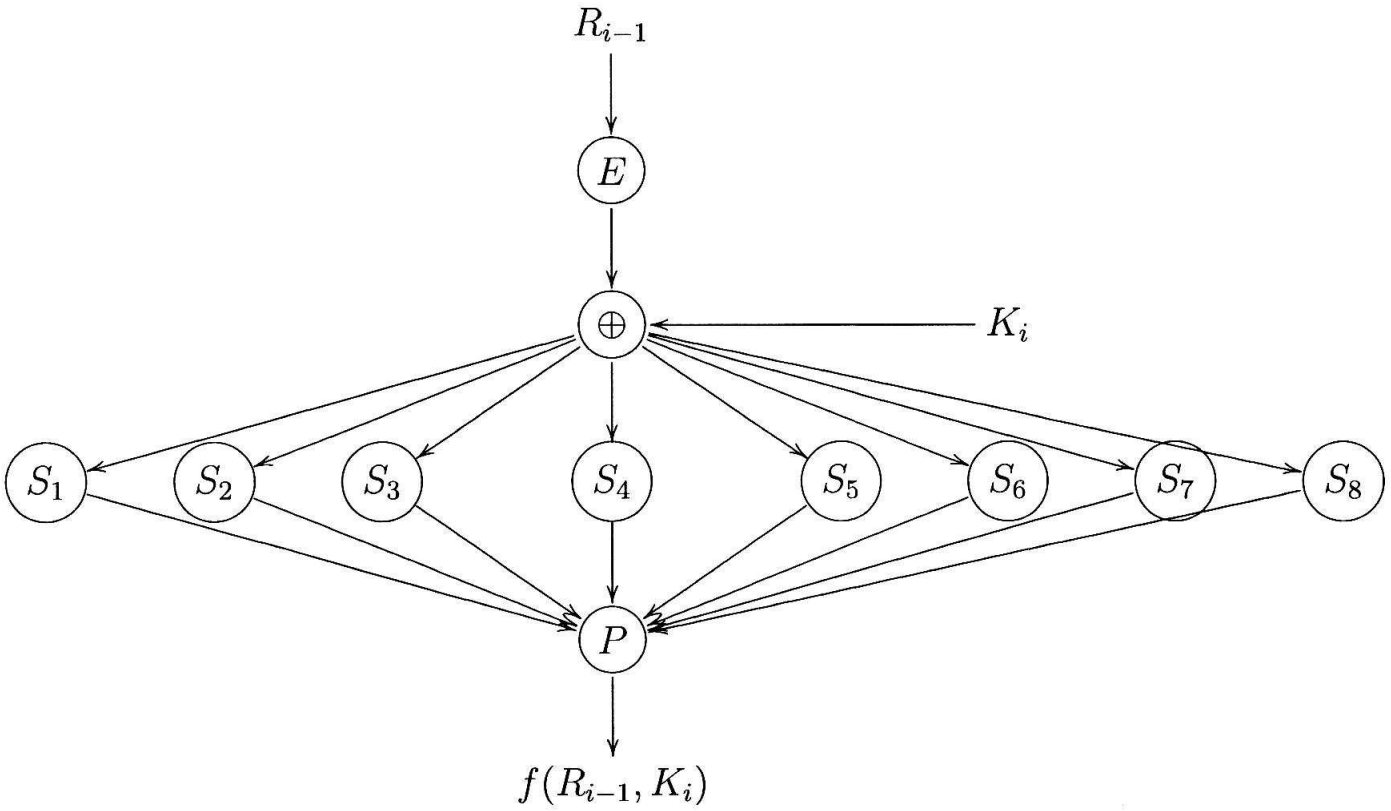
Data Encryption Standard I – Verschlüsselungsalgorithmus



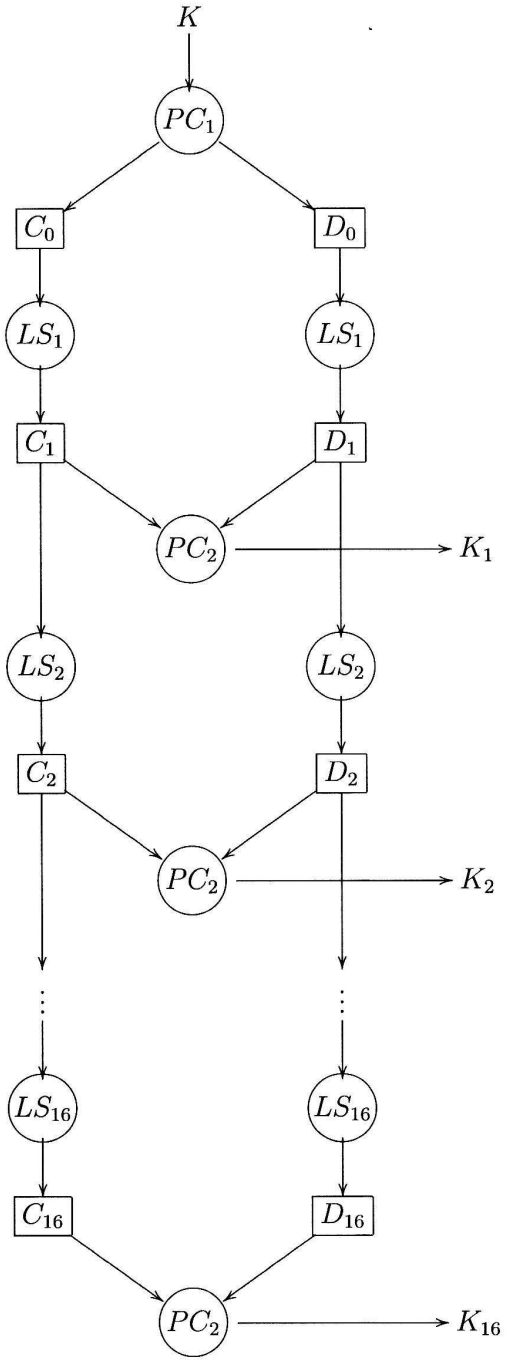
Data Encryption Standard II - Berechnungsschema von f



Data Encryption Standard III – Transformationen S_i

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S_1
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	9	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	S_2
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	S_3
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	S_4
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	8	14	9	S_5
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	S_6
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	S_7
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	S_8
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

Data Encryption Standard IV – Berechnung der K_i



Ein verschlüsselter Text III a

D E R I N D E R K A M V O R D E M

L E T T E N E R S A H D E N U N G

A R N U N D B E Z A H L T E D A S

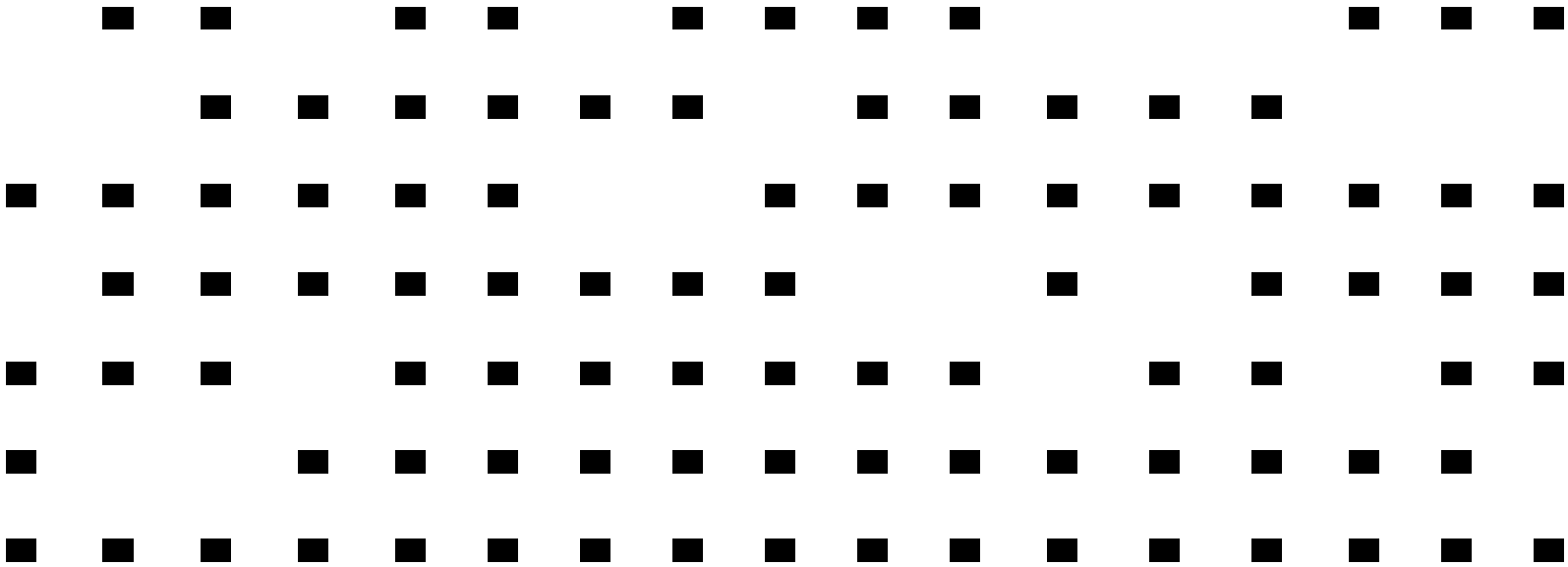
G E L D I M K L E I N E N R A U M

D E S T U R M E S A U F D E R B L

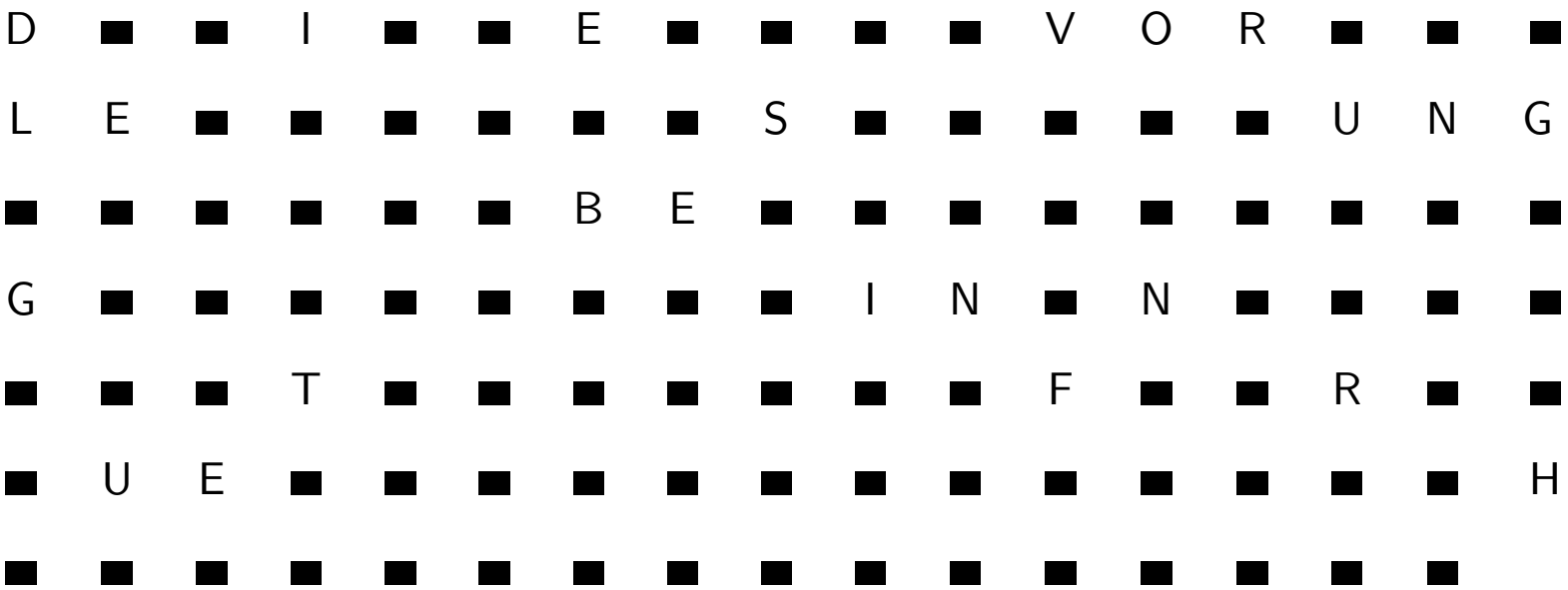
A U E N L I E G E S A S S D E R H

E S S E G E L A N G W E I L T

Ein verschlüsselter Text III b



Ein verschlüsselter Text III c



Perfekte Sicherheit

Definition: Wir sagen, dass die Verschlüsselungen aus $\mathcal{S}$ (bzw. die Schlüssel zu $\mathcal{S}$) hinsichtlich $\mathcal{T}$ und $\mathcal{K}$ perfekte Sicherheit bieten, falls

$$p_k(t) = p(t) \text{ für jeden Kryptotext } k \in \mathcal{K} \text{ und jeden Klartext } t \in \mathcal{T}$$

gilt.

Satz: Es sei $\mathcal{S}$ ein Schlüsselsystem mit $\#(\mathcal{T}) = \#(\mathcal{K}) = \#(\mathcal{S})$, in dem alle Schlüssel mit der gleichen Wahrscheinlichkeit vorkommen und in dem es zu jedem Klartext t und jedem Kryptotext k genau eine Transformation $\tau \in \mathcal{S}$ gibt, für die $\tau(t) = k$ gilt. Dann bietet $\mathcal{S}$ perfekte Sicherheit bez. $\mathcal{T}$ und $\mathcal{K}$.

Schieberegister

Definition:

i) Unter einem Schieberegister der Länge m verstehen wir

– m Speicherelemente k_1, k_2, . . . k_m, von denen jedes zu einem Zeitpunkt t, $t \geq 0$, genau ein Element $k_i(t) \in \{0, 1\}$ enthält,

– m Konstanten $c_1, c_2, \ldots, c_m$ aus $\{0, 1\}$ und

– m Werte $x_1, x_2, \ldots, x_m$ aus $\{0, 1\}$.

ii) Die Speicherelemente sind durch $k_i(0) = x_i$ für $1 \leq i \leq m$ initialisiert.

Die Veränderung in einem Speicherelement erfolgt taktweise entsprechend den folgenden Formeln:

– $k_1(t+1) = c_1k_1(t) \oplus c_2k_2(t) \oplus \ldots \oplus c_mk_m(t)$,

– $k_i(t+1) = k_{i-1}(t)$ für $2 \leq i \leq m,\ t \geq 0$.

iii) Die von einem Schieberegister ausgegebene Folge ist $k_t(0)k_t(1)k_t(2)\ldots$

Zwei Sätze

Satz.
Die Aufgabe des Kryptoanalysten, zu einem gegeben Kryptotext k den Klartext t zu finden, liegt in der Komplexitätsklasse NP (der nichtdeterministisch in polynomialer Zeit lösbaren Probleme).

Satz.
Wenn die Aufgabe des Kryptoanalysten NP-vollständig ist,
dann gilt NP=co-NP.

Super-Wachstum

Definition: i) Ein Vektor $(a_1, a_2, \ldots, a_n)$ heißt monoton wachsend, falls $a_i < a_{i+1}$ für $1 \leq i < n$ gilt.

ii) Ein Vektor $(a_1, a_2, \ldots, a_n)$ heißt super-wachsend, falls

$$\sum_{j=1}^{i-1} a_j < a_i$$

für $2 \leq i \leq n$ gilt.

Satz: Ist das Rucksack-Problem durch einen super-wachsenden Vektor A und a_{n+1} gegeben, so ist eine Lösung des Problems in linearer Zeit bestimmbar.

Modulare Multiplikation

Definition: Es seien der Vektor $A = (a_1, a_2, \ldots, a_n)$ gegeben. Ferner seien (t, m) ein Paar natürlicher Zahlen mit

$$ggT(t, m) = 1 \quad \text{und} \quad m > \max\{a_1, a_2, \ldots, a_n\}.$$

i) Wir sagen, dass der Vektor

$$B = (ta_1 \bmod m,\ ta_2 \bmod m,\ \ldots, ta_n \bmod m)$$

aus A durch modulare Multiplikation mit (t, m) entsteht. t und m heißen Faktor bzw. Modulus der modularen Multiplikation.

ii) Falls sogar $m > \sum_{i=1}^{n} a_i$ gilt, so sprechen wir von strenger modularer Multiplikation.

Eine Transformation

Satz:

Es seien A ein super-wachsender Vektor und b eine natürliche Zahl. Der Vektor B entstehe aus A durch strenge modulare Multiplikation mit (t, m).

i) Das Rucksack-Problem (B, b) besitzt höchstens eine Lösung.

ii) Wenn das Rucksack-Problem (B, b) eine Lösung besitzt, dann stimmt sie mit der Lösung von $(A, t^{-1}b)$ überein.

Super-Erreichbarkeit

Definition: Ein Vektor B heißt super-erreichbar, wenn es einen super-wachsenden Vektor A gibt, aus dem B mittels strenger modularer Multiplikation gewonnen werden kann.

Definition: Für einen Vektor $A = (a_1, a_2, \ldots a_n)$, eine natürliche Zahlen m und t mit $m \geq \max\{a_1, a_2, \ldots a_n\}$ und $ggT(t, m) = 1$ und eine natürliche Zahl $k \geq 0$ definieren den Vektor

$$A(k) = (a_1 + k\lfloor ta_1/m \rfloor, a_2 + k\lfloor ta_2/m \rfloor, \ldots, a_n + k\lfloor ta_n/m \rfloor)\,.$$

Die Folge der Vektoren $A(k)$, $k \geq 0$, heißt wachsende Folge zu A bez. (t, m).

Einige Aussagen I

Es seien $A = (a_1, a_2, \ldots a_n)$ ein Vektor und m und t natürliche Zahlen mit $m \geq \max\{a_1, a_2, \ldots a_n\}$ und $ggT(t, m) = 1$.

Lemma: Ist A ein (super-)wachsender Vektor, so ist auch jeder Vektor $A(k)$, $k \geq 0$, der wachsenden Folge bez. (m, t) (super-)wachsend.

Lemma: Falls der Vektor B durch eine modulare Multiplikation mit (t, m) aus dem Vektor A gewonnen werden kann. so entsteht B für jede natürliche Zahl $k \geq 0$ durch modulare Multiplikation mit $(t, kt + m)$ aus dem Vektor $A(k)$ der wachsenden Folge bez. (t, m). Diese Aussage gilt auch, wenn modulare Multiplikation durch strenge modulare Multiplikation ersetzt wird.

Einige Aussagen II

Lemma: Es seien $A = (a_1, a_2, \ldots a_n)$ ein Vektor und m und t natürliche Zahlen mit $m \geq \max\{a_1, a_2, \ldots a_n\}$ und $ggT(t, m) = 1$. Ferner sei B aus A mittels modularer Multiplikation mit (t, m) entstanden.

Dann gibt es genau dann ein $k \geq 0$ derart, dass B aus dem superwachsenden Vektor $A(k)$ der wachsenden Folge von A bez. (t, m) durch strenge modulare Multiplikation entsteht, wenn

$$\text{mit } m \leq \sum_{i=1}^{n} a_i \text{ auch } \sum_{i=1}^{n} \lfloor ta_i/m \rfloor < t \text{ gilt}$$

und

$$\text{für jedes } i,\ 1 \leq i \leq n, \text{ mit } a_i \leq \sum_{j=1}^{i-1} a_j \text{ auch } \sum_{j=1}^{i-1} \lfloor ta_j/m \rfloor < \lfloor ta_i/m \rfloor \text{ gilt.}$$

Einige Aussagen III

Lemma: Es seien $A = (a_1, a_2, \ldots a_n)$ ein Vektor und m und t natürliche Zahlen mit $m \geq \max\{a_1, a_2, \ldots a_n\}$ und $ggT(t, m) = 1$. Ferner sei B aus A mittels modularer Multiplikation mit (t, m) entstanden.

Falls B aus einem super-wachsenden Vektor $A(k)$ der wachsenden Folge von A bez. (t, m) durch strenge modulare Multiplikation entsteht, so sind alle $A(l)$ mit $l \geq \max\{z, z_1, z_2, \ldots, z_n\}$ super-wachsend und B entsteht aus jedem $A(l)$ durch strenge modulare Multiplikation.

Lemma: Der Vektor $B = (b_1, b_2, \ldots b_n)$ entstehe aus dem Vektor $A = (a_1, a_2, \ldots a_n)$ durch (strenge) modulare Multiplikation mit (t, m). Ferner seien

$A_1 = (\lfloor t_1 a_1/m_1 \rfloor, \lfloor t_1 a_2/m_1 \rfloor, \ldots, \lfloor t_1 a_n/m_1 \rfloor,\ t_1 = -m \bmod t$ und $m_1 = t$.

Falls $t < m$ und $t > \max\{b_1, b_2, \ldots b_n\}$ gilt, so entsteht B auch durch (strenge) modulare Multiplikation mit (t_1, m_1) aus A_1.

Einige Aussagen IV

Folgerung: Wenn $B = (b_1, b_2, \ldots b_n)$ super-erreichbar ist, dann entsteht B aus einem super-wachsenden Vektor A durch strenge modulare Multiplikator mit einem Faktor, der kleiner als $\max\{b_1, b_2, \ldots b_n\}$.

Definition: Es seien A ein Vektor und t und m natürliche Zahlen mit $ggT(t, m) = 1$. Wir definieren induktiv eine Folge von Vektoren $A(-k)$ durch folgende Setzungen:

— Es gilt $A(-0) = A$.

— Ist $A(-k) = (d_1, d_2, \ldots d_n)$ bereits definiert und gilt $m - kt > \max\{d_1, d_2, \ldots d_n\}$, so setzen wir

$$A(-k-1) = (d_1 - \lfloor td_1/(m-kt) \rfloor, d_2 - \lfloor td_2/(m-kt) \rfloor, \ldots, d_n - \lfloor td_n/(m-kt) \rfloor)\,.$$

Die Folge der $A(-k)$ heißt fallende Folge zu A bez. (t, m).

Einige Aussagen V

Lemma:

i) Ist der Vektor $A = (a_1, a_2, \ldots, a_n)$ monoton wachsend, dann sind auch die Vektoren $A(-k)$ jeder fallenden Folge zu A monoton wachsend.

ii) Ist $A(-k)$ ein Element der fallende Folge von A bez. (t, m). Dann ist A das k-te Elemente der wachsenden Folge von $A(-k)$ bez. $(t, m - kt)$.

Lemma:

Der Vektor $B = (b_1, b_2, \ldots b_n)$ resultiere aus A durch modulare Multiplikation mit (t, m), wobei

$$m > 2 \cdot \max\{b_1, b_2, \ldots b_n\} \text{ und } t \leq \max\{b_1, b_2, \ldots b_n\}$$

gelte. Dann resultiert B auch aus dem Vektor $A(-1)$ durch modulare Multiplikation mit $(t, m - t)$.

Einige Aussagen VI

Folgerung:

Wenn $B = (b_1, b_2, \ldots b_n)$ durch modulare Multiplikation aus einem Vektor entsteht, dann gibt es einen Vektor A aus dem B durch modulare Multiplikation mit (t, m) entsteht, wobei

$$t \leq \max\{b_1, b_2, \ldots b_n\} \text{ und } m \leq 2 \cdot \max\{b_1, b_2, \ldots b_n\}$$

gelten.

Einige Aussagen VII

Satz: Der Vektor $B = (b_1, b_2, \ldots b_n)$ ist genau dann super-erreichbar, wenn es einen monoton wachsenden Vektor A, natürliche Zahlen t und m mit $t \leq \max\{b_1, b_2, \ldots b_n\},\ m \leq 2 \cdot \max\{b_1, b_2, \ldots b_n\}$ und $ggT(t, m) = 1$ derart gibt, dass B aus A durch modulare Multiplikation mit (t, m) entsteht und A die Bedingung erfüllt, dass

$$\text{mit } m \leq \sum_{i=1}^{n} a_i \text{ auch } \sum_{i=1}^{n} \lfloor ta_i/m \rfloor < t \text{ gilt}$$

und

$$\text{für jedes } i,\ 1 \leq i \leq n, \text{ mit } a_i \leq \sum_{j=1}^{i-1} a_j \text{ auch } \sum_{j=1}^{i-1} \lfloor ta_j/m \rfloor < \lfloor ta_i/m \rfloor \text{ gilt.}$$

T0L-Systeme

Definition: Ein T0L-System ist ein Quadrupel $G = (V, \sigma_0, \sigma_1, w)$, wobei
– V ein Alphabet ist,
– σ_0 und $sigma_1$ endliche Substitutionen von V^* in V^* sind, und
– w ein nichtleeres Wort über V ist.

Ein T0L-System heißt DT0L-System, falls σ_0 und σ_1 Morphismen sind.

Satz: i) Das Parsing-Problem

Gegeben: T0L-System $G = (V, \sigma_0, \sigma_2, w)$ und $v \in V^*$
Gesucht: Binärwort $x \in \{0,1\}^*$ mit $v \in \sigma_G(x)$
(oder man treffe die Aussage, dass ein derartiges Wort nicht existiert)

ist **NP**-vollständig.

ii) Das Parsing-Problem ist für DT0L-Systeme in polynomialer Zeit lösbar.

Rückwärts eindeutige DT0L-Systeme

Definition: Ein DT0L-System $G = (V, h_0, h_1, w)$ heißt rückwärts eindeutig, wenn aus

$$h_{i_n}(h_{i_{n-1}}(\ldots(h_{i_1}(w))\ldots)) = h_{j_m}(h_{j_{m-1}}(\ldots(h_{j_1}(w))\ldots))$$

folgt, dass

$$m = n \quad \text{und} \quad i_k = j_k \text{ für } 1 \leq k \leq n$$

gelten.

Satz: Es ist algorithmisch nicht entscheidbar, ob ein gegebenes DT0L-System rückwärts eindeutig ist.

Einige Fakten I

Fakt 1.
Für zwei Primzahlen p und q möge $x = a \bmod p$ und $x = a \bmod q$ gelten. Dann gilt auch $x = a \bmod pq$.

Fakt 2.
i) Für n und m gelte $ggT(n, m) = 1$. Dann ist $\varphi(nm) = \varphi(n)\varphi(m)$.
ii) Für eine Primzahl p und eine beliebige natürliche Zahl $n \geq 1$ gilt $\varphi(p^n) = p^n - p^{n-1}$.

Fakt 3.
Für jede Primzahl p und jedes $a \in M_p$ gilt $a^{p-1} = 1 \bmod p$.

Fakt 4.
Für beliebige natürliche Zahlen $n \geq 2$ und $a \geq 1$ mit $ggT(a, n) = 1$ gilt die Beziehung $a^{\varphi(n)} = 1 \bmod n$.

Einige Fakten II

Fakt 5.
Für eine natürliche Zahl n sei $p(n)$ die Anzahl der Primzahlen, die $\leq n$ sind. Dann gilt

$$\lim_{n\to\infty} \left(p(n) - \frac{n}{\ln n}\right) = 0\,,$$

wobei $\ln$ den natürlich Logarithmus bedeutet.

Fakt 6.
i) Für zwei natürliche Zahlen n und m mit $n \geq m \geq 1$ lässt sich ihr größter gemeinsamer Teiler $ggT(n,m)$ in logarithmischer Zeit in n berechnen.
ii) Für natürliche Zahlen n und m mit $n \geq m \geq 1$ und $ggT(m,n) = 1$ lässt sich in logarithmischer Zeit in n eine Zahl a mit $ma = 1 \bmod n$ berechnen.

Zeugen für Primzahleigenschaft

Wir nennen eine Zahl u einen *Zeugen* dafür, dass eine Zahl m eine Primzahl ist, falls u die Bedingungen $ggT(u,m) = 1$ und $u^{m-1} = 1 \bmod m$ erfüllt.

Lemma:
Für eine gegebene Zahl $m \geq 2$ sind entweder alle Zahlen oder höchstens die Hälfte aller Zahlen u mit $1 \leq u \leq m-1$ und $ggt(u,m) = 1$ ein Zeuge dafür, dass m eine Primzahl ist.