Bernhard Dietrich

[b|d] bernhard dietrich

Mathematik für Informatiker I
Übungsblatt 10
Matrikel-Nr.: 6256800 · Übungsgruppe 1

Aufgabe 10.1

(i)

Klartext	B	E	R	N	H	A	R	D
x	1	4	17	13	7	0	17	3
$z \equiv ax + b \bmod 30$	2	11	19	7	20	30	19	9
Verschlüsselung	C	L	T	H	U	␣	T	J

(ii)

$$\left|\begin{array}{l} 9 \equiv 12a + b \bmod 31 \\ 11 \equiv 0a + b \bmod 31 \end{array}\right|$$

$$\Leftrightarrow \left|\begin{array}{l} 9 \equiv 12a + b \bmod 31 \\ 11 \equiv b \bmod 31 \end{array}\right|$$

$$\Leftrightarrow \left|\begin{array}{l} 9 \equiv 12a + 11 \bmod 31 \\ b \equiv 11 \bmod 31 \end{array}\right|$$

$$\Leftrightarrow \left|\begin{array}{l} -2 \equiv 12a \bmod 31 \\ b \equiv 11 \bmod 31 \end{array}\right|$$

$$\Leftrightarrow \left|\begin{array}{l} a \equiv -26 \bmod 31 \\ b \equiv 11 \bmod 31 \end{array}\right|$$

$$\Leftrightarrow \left|\begin{array}{l} a \equiv 5 \bmod 31 \\ b \equiv 11 \bmod 31 \end{array}\right|$$

(iii)

$$z \equiv 5x + 11 \bmod 31$$

$$\Leftrightarrow z - 11 \equiv 5x \bmod 31$$

$$\Leftrightarrow x \equiv 25z + 4 \bmod 31$$

Verschlüsselung	J	L	N	P	A	G	U	I	N	G	N	T	E	E
z	9	11	13	15	0	6	20	8	13	6	13	19	4	4
$x \equiv 25z + 4 \bmod 31$	12	0	19	7	4	30	8	18	19	30	19	14	11	11
Klartext	M	A	T	H	E	␣	I	S	T	␣	T	O	L	L

(iv) Unter der Vorraussetzung, dass m prim (und bekannt) ist, damit man in jedem Fall ein Inverses findet um das a zu isolieren zu können, benötigt man nur 2 Paare. Man will zwei Unbekannt (a, b) finden, also benötigt man ein Gleichungssystem mit 2 Gleichungen. Für die beiden Gleichungen benötigt man jeweils ein Buchstabenpaar um den verschlüsselten und den entschlüsselten Wert des Buchstabens einsetzen zu können.

$$\left| \begin{array}{l} z_1 \equiv x_1 a + b \bmod m \\ z_2 \equiv x_2 a + b \bmod m \end{array} \right|$$

$$\Leftrightarrow \quad \left| \begin{array}{l} z_1 \equiv x_1 a + b \bmod m \\ z_2 - z_1 \equiv (x_2 - x_1)\, a \bmod m \end{array} \right| \text{(II-I)}$$

$$\Leftrightarrow \quad \left| \begin{array}{l} z_1 \equiv x_1 a + b \bmod m \\ a \equiv (z_2 - z_1)(x_2 - x_1)^{-1} \bmod m \end{array} \right|$$

$$\Leftrightarrow \quad \left| \begin{array}{l} z_1 \equiv x_1 \left((z_2 - z_1)(x_2 - x_1)^{-1}\right) + b \bmod m \\ a \equiv (z_2 - z_1)(x_2 - x_1)^{-1} \bmod m \end{array} \right|$$

$$\Leftrightarrow \quad \left| \begin{array}{l} b \equiv z_1 - x_1 \left((z_2 - z_1)(x_2 - x_1)^{-1}\right) \bmod m \\ a \equiv (z_2 - z_1)(x_2 - x_1)^{-1} \bmod m \end{array} \right|$$

Aufgabe 10.2

$U = \{x \mid x \notin x\}$

Die Aussage ist paradox. U ist gleich der Menge aller Mengen x, die sich nicht selbst enthält.
Ist x nicht enthalten, muss es enthalten sein, ist x aber enthalten, darf es nicht enthalten sein.
Daher müsste in diesem Fall sowohl $U \in U$ als auch $U \notin U$ gelten.
Ein Beispiel für einen solchen Fall ist ein Verzeichnis aller Bücherverzeichnisse, die sich nicht selbst auflisten.
Russel zeigte, dass der Mengenbegriff von Cantor nicht exakt genug ist, da er Mengendefinitionen erlaubt, für die die Elementbeziehung nicht entschieden werden kann.
Dieses Dilemma konnte erst durch Einführung der Axiomatischen Mengenlehre behoben werden, die die Definition von Mengen einschränkt. Meist wird das Axiomensystem von Zermelo und Fränkel verwendet.

Aufgabe 10.3

(i) $P \setminus Q = \{1, 5\}$

(ii) $P \cup Q = \{1, 2, 4, 5\}$

(iii) $P \times Q = \{(1,2), (1,4), (4,2), (4,4), (5,2), (5,4)\}$

(iv) $U \setminus S = \{x \in \mathbb{N} : x < 44 \wedge 3 \nmid x\}$

(v) $U \setminus T = \{x \in \mathbb{N} : x < 40\}$

(vi) $S \cap T \cap U = \{42\}$

Aufgabe 10.4

$$
\begin{aligned}
S \cap (T \cup V) &\Leftrightarrow x \in S \cap (T \cup V) \\
&= x \in S \wedge x \in (T \cup V) \\
&= x \in S \wedge (x \in T \vee x \in V) \\
&= (x \in S \wedge x \in T) \vee (x \in S \wedge x \in V) \\
&= x \in (S \cap T) \vee x \in (S \cap V) \\
&= x \in (S \cap T) \cup (S \cap V) \\
&\Leftrightarrow (S \cap T) \cup (S \cap V)
\end{aligned}
$$

Aufgabe 10.5

Angenommen, es gibt keine Person, die alle Personen kennt (sich selber eingeschlossen) und es gibt keine Person, die keinen kennt.
Dann hat Person 1 einen Bekannten, Person 2 zwei Bekannte, usw. Person n-1 hat dann n-1 Bekannte.
Da Person n nicht n Bekannte haben kann (siehe oben) und auch nicht 0 Bekannte, muss sie eine Bekanntenanzahl zwischen 1 und n-1 haben. Da es aber für jede Bekanntenanzahl bereits eine Person gibt, die so viele Leute kennt, müssen zwei Personen gleich viele Bekannte haben.