10. Musterlösung zu Mathematik für Informatiker I, WS 2003/04

KATHRIN TOFALL

Aufgabe 10.1 (Affine Chiffren). (4 Punkte)

Für diese Aufgabe verwenden wir das Alphabet mit den Buchstaben `A` bis `Z`, `Ä`, `Ö`, `Ü`, dem Bindestrich `-` und dem Leerzeichen `␣`. In dieser Reihenfolge sind die Zeichen den Elementen $0, \ldots, 30$ von $\mathbb{Z}_{31}$ zugeordnet. Zum Beispiel entspricht `E` also 4 und `-` der 29, das Leerzeichen der 30.

Bei *affinen Codes* wird ein Zeichen $x \in \mathbb{Z}_m$ durch $ax + b$ ersetzt, wobei $a \in \mathbb{Z}_m^\times$, $b \in \mathbb{Z}_m$. Wir verwenden hier $m = 31$. *Beispiel*: Sei $a = 2$, $b = 1$.

Klartext	J	A	N	-	F	E	L	I	X
Verschlüsselung	T	B	Ö	Ü	L	J	X	R	Q

(i) Verschlüssele die bis zu 10 ersten Zeichen Deines Vornamens mit $a = 3$, $b = 30$. 1

Lösung. Wir berechnen also für alle verwendeten Zeichen z: $3z + 30 \equiv 3z - 1 \bmod 31$. Bei dem Beispielnamen „Jan-Felix" würde also wie folgt verschlüsselt:

$$
\begin{array}{llllllllllll}
\text{„J"} & \triangleq & 9 & \mapsto & 3 \cdot & 9 & - & 1 & \equiv_{31} & 26 & \triangleq & \text{„Ä"}, \\
\text{„A"} & \triangleq & 0 & \mapsto & 3 \cdot & 0 & - & 1 & \equiv_{31} & 30 & \triangleq & \text{„␣"} \\
\text{„N"} & \triangleq & 13 & \mapsto & 3 \cdot & 13 & - & 1 & \equiv_{31} & 7 & \triangleq & \text{„H"}, \\
\text{„-"} & \triangleq & 29 & \mapsto & 3 \cdot & (-2) & - & 1 & \equiv_{31} & 24 & \triangleq & \text{„Y"}, \\
\text{„F"} & \triangleq & 5 & \mapsto & 3 \cdot & 5 & - & 1 & \equiv_{31} & 14 & \triangleq & \text{„O"}, \\
\text{„E"} & \triangleq & 4 & \mapsto & 3 \cdot & 4 & - & 1 & \equiv_{31} & 11 & \triangleq & \text{„L"}, \\
\text{„L"} & \triangleq & 11 & \mapsto & 3 \cdot & 11 & - & 1 & \equiv_{31} & 1 & \triangleq & \text{„B"}, \\
\text{„I"} & \triangleq & 8 & \mapsto & 3 \cdot & 8 & - & 1 & \equiv_{31} & 23 & \triangleq & \text{„X"}, \\
\text{„X"} & \triangleq & 23 & \mapsto & 3 \cdot & (-8) & - & 1 & \equiv_{31} & 6 & \triangleq & \text{„G"}.
\end{array}
$$

Somit also:

Klartext	J	A	N	-	F	E	L	I	X
Verschlüsselung	Ä	␣	H	Y	O	L	B	X	G

○

Du hast einen verschlüsselten Text abgefangen: `JLNPAGUINGNTEE`. Später erfährst Du (durch einen Spion), dass der Klartext mit `MAT` anfängt.

(ii) Bestimme a und b. [1]

Lösung. Wir wissen ja, dass `M` zu `J` wird, `A` zu `L` und `T` zu `N`. Außerdem ist $m = 31$. Also haben wir folgende Gleichungen:

$$\begin{aligned} 9 &\equiv 12a + b \bmod 31 \\ 11 &\equiv b \bmod 31 \\ 13 &\equiv 19a + b \bmod 31. \end{aligned}$$

b ist also sofort bekannt:

$$b \equiv 11 \bmod 31.$$

Mithilfe des EEA können wir jetzt 12 oder 19 modulo 31 invertieren (je nach dem, mit welcher Gleichung wir b berechnen wollen):

$$12^{-1} \equiv 13 \bmod 31 \text{ und } 19^{-1} \equiv 18 \bmod 31.$$

Da $b \equiv 11 \bmod 31$ sehen die beiden übrigen Gleichungen nach dem Einsetzen so aus:

$$12a \equiv -2 \bmod 31 \text{ und } 19a \equiv 2 \bmod 31.$$

Multipliziert mit dem jeweils zugehörigen Inversen erhalten wir:

$$a \equiv -26 \equiv 5 \bmod 31 \text{ und } a \equiv 36 \equiv 5 \bmod 31.$$

Damit sind a und b bestimmt und die gesuchte Verschlüsselungsgleichung ist

$$5x + 11 \bmod 31.$$

Bemerkung: Man hätte natürlich nicht über beide Gleichungen a berechnen müssen, aber man kann das selbstverständlich mit jeder der beiden. ○

[1] (iii) Entschlüssele den Rest der Nachricht.

Lösung. Zum Entschlüsseln der Nachricht, müssen wir die Verschlüsselungsgleichung umkehren. Wir wissen inzwischen, dass ein verschlüsseltes Zeichen y dem Wert von $5x + 11 \bmod 31$ entspricht, wobei x das Klartextzeichen ist. Also

$$y \equiv 5x + 11 \bmod 31.$$

Wenn wir zurückrechnen wollen, brauchen wir also

- das additive Inverse von 11 modulo 31 — das ist einfach $-11 \equiv 20 \bmod 31$ und
- das multiplikative Inverse von 5 modulo 31 — das können wir wieder mit dem EEA bestimmen und es gilt $\frac{1}{5} \equiv 25 \bmod 31$.

Also gilt

$$x \equiv 25 \cdot (y - 11) \equiv -6y + 66 \equiv -6y + 4.$$

Damit können wir jetzt den verschlüsselten Text lesen:

Verschlüsselung	J	L	N	P	A	G	U	I	N	G	N	T	E	E
Klartext	M	A	T	H	E	␣	I	S	T	␣	T	O	L	L

◯

In der allgemeinen Situation sind einige Paare aus Klartext- und Schlüsselbuchstabe bekannt.

(iv) Wieviele solche Paare (mit unterschiedlichen Klartextbuchstaben) brauchst Du, um a und b zu bestimmen zu können? Beweise. 1

Lösung. Wir brauchen zwei unterschiedliche Paare, wenn unser m bekannt und prim ist. Sei also m prim und die Paare diese

$$y_1 \equiv ax_1 + b \bmod m \text{ und } y_2 \equiv ax_2 + b \bmod m.$$

Wenn wir jetzt die beiden Gleichungen von einander abziehen, erhalten wir: $y_1 - y_2 \equiv ax_1 - ax_2 = a(x_1 - x_2) \bmod m$. Da m prim ist, kann $x_1 - x_2$ auf jeden Fall invertiert werden, somit gilt dann

$$a \equiv (y_1 - y_2) \cdot (x_1 - x_2)^{-1} \bmod m.$$

Den Wert für a können wir in eine der beiden Ausgangsgleichungen einsetzen:

$$b \equiv y_1 - ax_1 \equiv y_1 - (y_1 - y_2)(x_1 - x_2)^{-1}x_1.$$

Also ist die Verschlüsselungsgleichung

$$y \equiv \frac{y_1 - y_2}{x_1 - x_2}x + y_1 - \frac{y_1 - y_2}{x_1 - x_2}x_1 \bmod 31.$$

Entsprechend ist die Entschlüsselungsgleichung dann

$$x \equiv \frac{x_1 - x_2}{y_1 - y_2} \cdot \left(y - y_1 + \frac{y_1 - y_2}{x_1 - x_2}x_1\right) \bmod 31.$$

◯

Aufgabe 10.2 (Russelsche Antinomie). (2 Punkte)

Betrachte die Menge

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

Gilt $\mathcal{U} \in \mathcal{U}$ oder $\mathcal{U} \notin \mathcal{U}$?

Lösung. $\mathcal{U}$ enthält alles bis auf Mengen, die sich selbst enthalten.

Nehmen wir zunächst an, es wäre $\mathcal{U} \in \mathcal{U}$. Dann folgt aber sofort $\mathcal{U} \notin \mathcal{U}$ im Widerspruch zur Annahme.

Nehmen wir jetzt aber an, $\mathcal{U} \notin \mathcal{U}$. Wiederum mit der Definition von $\mathcal{U}$ folgt $\mathcal{U} \in \mathcal{U}$, also wieder ein Widerspruch zur Annahme.

Somit gilt weder $\mathcal{U} \in \mathcal{U}$ noch $\mathcal{U} \notin \mathcal{U}$. ◯

Das ist mathematisch gesehen natürlich ein Dilemma, denn eine Aussage oder ihre Verneinung sollte wahr sein. Daher muss irgendwo ein Problem liegen: die einzige mögliche Stelle ist die Definition von $\mathcal{U}$. Wir haben einfach nicht richtig gesagt, woher die Elemente von $\mathcal{U}$ stammen sollen. Wenn die Kandidaten x einfach alle Mengen sind, dann ist diese zusätzliche Bedingung vielleicht der Ausweg. Es stellt sich dann nämlich zuerst die Frage: Ist $\mathcal{U}$ eine Menge? Die Antwort darauf muss „Nein!“ lauten. Dann ist der Widerspruch bereinigt und unsere Welt wieder in Ordnung, wenn auch etwas komplizierter als wir vielleicht zuerst dachten.

Aufgabe 10.3 (Mengenoperationen). (3 Punkte)

Sei $P = \{1, 4, 5\}$, $Q = \{2, 4\}$, $S = \{x \in \mathbb{N} : 3 \mid x\}$,
$T = \{x \in \mathbb{N} :$ Die Zehnerziffer von x ist $4.\}$, $U = \{x \in \mathbb{N} : x < 44\}$. Bestimme

(i) $P \setminus Q$,

(ii) $P \cup Q$,

(iii) $P \times Q$,

(iv) $U \setminus S$,

(v) $U \setminus T$,

(vi) $S \cap T \cap U$.

Lösung. (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 (Mengen). (2 Punkte)

Seien S, T und V Mengen. Zeige, dass gilt: $S \cap (T \cup V) = (S \cap T) \cup (S \cap V)$.

Lösung. Sei $x \in S \cap (T \cup V)$. Dann gilt

$$(x \in S) \wedge ((x \in T) \vee (x \in V)) .$$

Das kann umgeformt werden zu

$$(x \in S) \wedge (x \in T) \ \vee \ (x \in S) \wedge (x \in V),$$

was bedeutet: $x \in (S \cap T) \cup (S \cap V)$. ◯

Aufgabe 10.5 (Bekannte). (2 Punkte)

Neulich behauptete eine Mathe-für-Informatiker-1-Studentin, dass es im Hörsaal zwei Personen gäbe, die gleichviele Bekannte unter den Leuten im Hörsaal haben. Was meinst Du dazu?

Lösung. Die Aussage ist wahr. Sei die Anzahl der Studenten in der Vorlesung gleich n. Dann kann jeder der n Studenten zwischen 0 und $n-1$ Bekannte dort haben. Das sind n Möglichkeiten. Da es aber nicht möglich ist, dass einer der Studenten niemanden in der Vorlesung (0 Bekannte) und gleichzeitig ein anderer Student alle seine Komillitonen ($n-1$ Bekannte) kennt, bleiben noch höchstens $n-1$ Möglichkeiten für Anzahlen an Bekannten für n Studenten, nämlich $\{0, \ldots, n-2\}$, falls tatsächlich jemand dabei ist, der niemanden kennt, und $\{1, \ldots, n-1\}$ andernfalls. Somit müssen zwei Studenten die gleiche Anzahl an Bekannten haben. ◯