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

JOACHIM VON ZUR GATHEN, OLAF MÜLLER-TOFALL, MICHAEL NÜSKEN

Abgabe bis Freitag, 16. Januar 2004, 11^{11}
in den jeweils richtigen grünen oder roten Kasten auf dem D1-Flur.

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 $a = 3$, $b = 30$.

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

(ii) Bestimme a und b.

(iii) Entschlüssele den Rest der Nachricht.

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.

Aufgabe 10.2 (Russelsche Antinomie). (2 Punkte)

Betrachte die Menge

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

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

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) $S \cap T \cap U$.

Aufgabe 10.4 (Mengen). (2 Punkte)

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

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?

10. Übungsblatt zu Mathematik für Informatiker I, WS 2003/04, Mündlicher Teil

JOACHIM VON ZUR GATHEN, OLAF MÜLLER-TOFALL, MICHAEL NÜSKEN

Mündliche Aufgabe 10.6 (Affine Chiffren).

Für diese Aufgabe verwenden wir das Alphabet mit den Buchstaben `A` bis `Z`. In dieser Reihenfolge sind die Zeichen den Elementen $0, \ldots, 25$ von $\mathbb{Z}_{26}$ zugeordnet. Zum Beispiel entspricht `F` also 5 und `X` der 23.

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 $m = 26$. *Beispiel*: Sei $a = 3$, $b = 5$.

Klartext	K	A	R	L	X	J	O	E	R	G
Verschlüsselung	J	F	E	M	W	G	V	R	E	X

Die Umlaute werden hier aufgelöst, da keine Extrazeichen für sie reserviert sind. Das `X` ist in dem Namen, weil wir keinen Bindestrich und kein Leerzeichen haben, in dem Fall kann man zur Trennung der Worte eben z.B. einen selten vorkommenden Buchstaben verwenden.

(i) Verschlüssele die bis zu 6 ersten Zeichen Deines Vornamens mit $a = 7$, $b = 21$.

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

(ii) Bestimme a und b.

(iii) Entschlüssele den Rest der Nachricht.

(iv) Verschlüssele das Wort `OK` mit $a = 13$ und $b = 4$. Was passiert beim Entschlüsseln? Erkläre Deine Beobachtung!

(v) Das Wort `KO` wurde zu `RN` verschlüsselt. Was passiert hier beim Entschlüsseln? Erkläre Deine Beobachtung!

Mündliche Aufgabe 10.7 (Mengenoperationen).

Sei $P = \{1, 3, 7\}$, $Q = \{3, 4\}$, $S = \{x \in \mathbb{N} : x \bmod 10 = 7\}$,
$T = \{x \in \mathbb{N} : \text{Die Quersumme von } x \text{ ist } 5.\}$, $U = \{x \in \mathbb{N} : x < 23\}$. Bestimme

(i) $P \setminus Q$,

(ii) $P \cup U$,

(iii) $P \times Q$,

(iv) $U \setminus S$,

(v) $U \setminus T$,

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

Mündliche Aufgabe 10.8 (Mengen).

Seien S, T und V Mengen. Gilt $S \setminus (T \cup V) = (S \setminus T) \cup (S \setminus V)$?

Mündliche Aufgabe 10.9 (Maus).

Ein Käsewürfel ist in 27 kleine Würfel eingeteilt. Eine Maus beginnt an einer Ecke und isst alle kleinen Würfel, als nächsten immer einen der direkt neben dem letzten liegt. Kann sie in der Mitte aufhören?