Prof. Dr. Sven Kosub / Michael Aichem, Julian Müller, Dagmar Sorg, Michael Strecke, Nadja Willenborg

# 1. Übungsblatt
# (Musterlösung)

**Ausgabe:** 17.04.2015 **Abgabe:** 24.04.2015, bis spätestens 12:00 per Mail an den Tutor

## Vertiefung: 10 Punkte

(a) Bestimmen Sie $\mathrm{mod}\left(5^{31}\cdot 2^{789}-23^{23},10\right)$.

(b) Bestimmen Sie $\mathrm{mod}\left(5^{31}\cdot 2^{789}-23^{23},11\right)$.

(c) Bestimmen Sie $\mathrm{mod}\left(7^{31}\cdot 2^{789},10\right)$.

(d) Bestimmen Sie $\mathrm{kgV}(178,144)$.

(e) Bestimmen Sie $\mathrm{ggT}(12877480,24145275)$.

(f) Wie sieht der zu $\frac{12877480}{24145275}$ äquivalente teilerfremde Bruch aus?

(g) Wie viele Funktionen $f:\{0,1,2,3\}^n\to\{0,1,2\}$ gibt es, die genau einmal den Funktionswert 0 annehmen?

(h) Wie viele Funktionen $f:\{0,1,2,3\}^n\to\{0,1,2\}$ gibt es, die genau zweimal den Funktionswert 0 annehmen?

(i) Wie viele Funktionen $f:\{0,1,2,3\}^n\to\{0,1,2\}$ gibt es, die genauso oft die Funktionswerte 0 und 1 annehmen?

(j) Wie viele Funktionen $\varphi:\mathcal{P}(A)\to\{\ f\mid f:\{0,1\}\to A\ \}$ gibt es, wenn $A$ eine endliche Menge ist?

*Hinweis:* Benutzen Sie auch das Skriptum *Brückenkurs Mathematik*.

## Lösung:

(a) Wegen $\mathrm{mod}(10,10)=0$ und $\mathrm{mod}(3^4,10)=1$ erhalten wir mit den Regeln der Modulo-Arithmetik:

$$\begin{aligned}
&\mathrm{mod}\left(5^{31}\cdot 2^{789}-23^{23},10\right)\\
&= \mathrm{mod}\left(10^{31}\cdot 2^{758}+\mathrm{mod}(-1,10)\cdot 23^{23},10\right)\\
&= \mathrm{mod}\left(\mathrm{mod}(10,10)^{31}\cdot 2^{758}+9\cdot \mathrm{mod}(23,10)^{23},10\right)\\
&= \mathrm{mod}\left(3^2\cdot 3^{23},10\right)\\
&= \mathrm{mod}\left(3^{4\cdot 6+1},10\right)\\
&= \mathrm{mod}\left(\mathrm{mod}(3^4,10)^6\cdot \mathrm{mod}(3,10),10\right)\\
&= 3
\end{aligned}$$

(b) Mit den Regeln der Modulo-Arithmetik erhalten wir zunächst:

$$\begin{aligned}
\mathrm{mod}(2^1, 11) &= \mathrm{mod}(2, 11) = 2\\
\mathrm{mod}(2^2, 11) &= \mathrm{mod}(4, 11) = 4\\
\mathrm{mod}(2^3, 11) &= \mathrm{mod}(8, 11) = 8\\
\mathrm{mod}(2^4, 11) &= \mathrm{mod}(16, 11) = 5\\
\mathrm{mod}(2^5, 11) &= \mathrm{mod}(10, 11) = 10\\
\mathrm{mod}(2^6, 11) &= \mathrm{mod}(20, 11) = 9\\
\mathrm{mod}(2^7, 11) &= \mathrm{mod}(18, 11) = 7\\
\mathrm{mod}(2^8, 11) &= \mathrm{mod}(14, 11) = 3\\
\mathrm{mod}(2^9, 11) &= \mathrm{mod}(6, 11) = 6\\
\mathrm{mod}(2^{10}, 11) &= \mathrm{mod}(12, 11) = 1
\end{aligned}$$

Außerdem gilt $\mathrm{mod}(100, 11) = 1$. Daraus ergibt sich:

$$\begin{aligned}
&\mathrm{mod}\left(5^{31} \cdot 2^{789} - 23^{23}, 11\right)\\
&= \mathrm{mod}\left(10^{31} \cdot 2^{758} - 23^{23}, 11\right)\\
&= \mathrm{mod}\left(10^{2\cdot 15+1} \cdot 2^{10\cdot 75+8} - (23, 11)^{23}, 11\right)\\
&= \mathrm{mod}\left(\mathrm{mod}(100, 11)^{15} \cdot 10 \cdot \mathrm{mod}(2^{10}, 11)^{75} \cdot \mathrm{mod}(2^8, 11) - \mathrm{mod}(23, 11)^{23}, 11\right)\\
&= \mathrm{mod}\left(10 \cdot \mathrm{mod}(2^8, 11) - 1, 11\right)\\
&= 7
\end{aligned}$$

(c) Um $\mathrm{mod}(2^5, 10) = 2$ geeignet anzuwenden, schreiben wir 789 wie folgt:

$$\begin{aligned}
789 &= 5 \cdot 157 + 4\\
&= 5 \cdot (5 \cdot 31 + 2) + 4\\
&= 5 \cdot (5 \cdot (5 \cdot 6 + 1) + 2) + 4\\
&= 5 \cdot (5 \cdot (5 \cdot (5 + 1) + 1) + 2) + 4
\end{aligned}$$

Durch wiederholte Anwendung von $\mathrm{mod}(2^5, 10) = 2$ ergibt sich zunächst:

$$\begin{aligned}
\mathrm{mod}(2^{789}, 10) &= \mathrm{mod}(2^{157} \cdot 2^4, 10)\\
&= \mathrm{mod}(2^{31} \cdot 2^2 \cdot 2^4, 10)\\
&= \mathrm{mod}(2^6 \cdot 2^1 \cdot 2^2 \cdot 2^4, 10)\\
&= \mathrm{mod}(2 \cdot 2^1 \cdot 2^1 \cdot 2^2 \cdot 2^4, 10)\\
&= \mathrm{mod}(2^9, 10)\\
&= 2
\end{aligned}$$

Außerdem gilt $\mathrm{mod}(7^4, 10) = \mathrm{mod}(9^2, 10) = 1$. Damit erhalten wir:

$$\begin{aligned}
&\mathrm{mod}\left(7^{31} \cdot 2^{789}, 10\right)\\
&= \mathrm{mod}\left(7^{4\cdot 7+3} \cdot 2, 10\right)\\
&= \mathrm{mod}\left(\mathrm{mod}(7^4, 10)^7 \cdot \mathrm{mod}(7^3, 10) \cdot 2, 10\right)\\
&= \mathrm{mod}\left(1^7 \cdot 3 \cdot 2, 10\right)\\
&= 6
\end{aligned}$$

(d) Es gilt $178 = 2 \cdot 89$ und $144 = 2^4 \cdot 3^2$. Mithin gilt $\mathrm{kgV}(178, 144) = 144 \cdot 89 = 12816$

(e) Durch Anwendung des Algorithmus von Euklid ergibt sich:

$$\begin{aligned} \mathrm{ggT}(12877480, 24145275) &= \mathrm{ggT}(11267795, 12877480) \\ &= \mathrm{ggT}(1609685, 11267795) \\ &= 1609685 \end{aligned}$$

(f) Es gilt:

$$\frac{12877480}{24145275} = \frac{\frac{12877480}{\mathrm{ggT}(12877480,24145275)}}{\frac{24145275}{\mathrm{ggT}(12877480,24145275)}} = \frac{\frac{12877480}{1609685}}{\frac{24145275}{1609685}} = \frac{8}{15}$$

(g) Es stehen $4^n$ verschiedene Argumente zur Verfügung, die auf den Funktionswert 0 abgebildet werden können; die restlichen $4^n - 1$ Argumente müssen auf die Funktionswerte $1, 2$ abgebildet werden. Somit gibt es nach der Potenzregel

$$4^n \cdot 2^{4^n - 1}$$

derartige Funktionen.

(h) Es gibt $\binom{4^n}{2}$ Möglichkeiten, zwei Argumente auf den Funktionswert 0 abzubilden; die restlichen $4^n - 2$ Argumente müssen auf die Funktionswerte $1, 2$ abgebildet werden. Somit gibt es nach Potenzregel

$$\binom{4^n}{2} \cdot 2^{4^n - 2}$$

derartige Funktionen.

(i) Für $k \in \{0, 1, \ldots, 2^{2n-1}\}$ gibt es $\binom{4^n}{2k}\binom{2k}{k}$ Funktionen, die genau $k$ Funktionswerte 0 und genau $k$ Funktionswerte 1 aufweisen: Wir ählen $2k$ Argumente aus $4^n$ möglichen aus; von diesen $2k$ Argumenten werden wiederum $k$ ausgewählt, die auf 0 abgebildet werden, die anderen $k$ werden auf 1 abgebildet. Somit ist die Gesamtzahl derartiger Funktionen:

$$\sum_{k=0}^{2^{2n-1}} \binom{4^n}{2k}\binom{2k}{k}$$

(j) Es gilt $\|\mathcal{P}(A)\| = 2^{\|A\|}$ sowie $\|\{\, f \mid f : \{0, 1\} \to A \,\}\| = \|A\|^2$. Somit gibt es

$$\left(\|A\|^2\right)^{2^{\|A\|}} = \|A\|^{2^{\|A\|+1}}$$

derartige Funktionen.

**Kreativität:** **10 Punkte**

Die *dyadische Kodierung* natürlicher Zahlen ist die wie folgt rekursiv definierte, bijektive Abbildung $\mathrm{dya} : \mathbb{N} \to \{1, 2\}^*$:

$$\begin{aligned} \mathrm{dya}(0) &=_{\mathrm{def}} \varepsilon \\ \mathrm{dya}(2n+1) &=_{\mathrm{def}} \mathrm{dya}(n)1 \\ \mathrm{dya}(2n+2) &=_{\mathrm{def}} \mathrm{dya}(n)2 \end{aligned}$$

$\{1,2\}^*$ steht für die Menge aller Wörter endlicher Länge, die mit den Buchstaben (Ziffern) 1 und 2 gebildet werden können, und $\varepsilon$ steht für das leere Wort (das Wort der Länge 0).

Zum Beispiel gilt $\mathrm{dya}(17) = \mathrm{dya}(8)1 = \mathrm{dya}(3)21 = \mathrm{dya}(1)121 = \mathrm{dya}(0)1121 = 1121$.

Zeigen Sie mittels vollständiger Induktion über die Länge $n$ der Code-Wörter, dass für die Umkehrabbildung $\mathrm{dya}^{-1} : \{1,2\}^* \to \mathbb{N}$ gilt:

$$\mathrm{dya}^{-1}(a_{n-1}\dots a_1 a_0) = \sum_{k=0}^{n-1} a_k \cdot 2^k$$

**Lösung:** Wir führend einen Induktionsbeweis über die Anzahl $n$ der Buchstaben von Code-Wörtern $a_{n-1}\dots a_1 a_0$.

- *Induktionsanfang*: Es sei $n = 0$. Somit ist das Code-Wort gerade das leere Wort $\varepsilon$. Mithin gilt die Aussage wegen $\mathrm{dya}^{-1}(\varepsilon) = 0$.
- *Induktionsschritt*: Es sei $n > 0$. Für ein Code-Wort $z = a_{n-1}\dots a_1 a_0$ ist $z' = a_{n-1}\dots a_1$ ein Code-Wort der Länge $n-1$. Für $z'$ kann die Induktionsvoraussetzung

$$\mathrm{dya}^{-1}(a_{n-1}\dots a_1) = \sum_{k=0}^{n-2} a_{k+1} \cdot 2^k$$

angewendet werden. Wegen $\mathrm{dya}\left(2 \cdot \mathrm{dya}^{-1}(z') + a_0\right) = z' a_0 = z$ gilt

$$\mathrm{dya}^{-1}(a_{n-1}\dots a_1 a_0) = 2 \cdot \mathrm{dya}^{-1}(a_{n-1}\dots a_1) + a_0$$

und wir erhalten:

$$\begin{aligned}
\mathrm{dya}^{-1}(a_{n-1}\dots a_1 a_0) &= 2 \cdot \mathrm{dya}^{-1}(a_{n-1}\dots a_1) \quad + a_0 \\
&= 2 \cdot \sum_{k=0}^{n-2} a_{k+1} \cdot 2^k \quad + a_0 \qquad \text{(nach Induktionsvoraussetzung)} \\
&= \sum_{k=0}^{n-2} a_{k+1} \cdot 2^{k+1} \quad + a_0 \\
&= \sum_{k=1}^{n-1} a_k \cdot 2^k \quad + a_0 \cdot 2^0 \\
&= \sum_{k=0}^{n-1} a_k \cdot 2^k
\end{aligned}$$

Damit ist die Aussage bewiesen.

**Transfer:** **10 Punkte**

Sie haben die Aufgabe, für ein Rechenzentrum einen Leitfaden mit Empfehlungen für die Erstellung hochsicherer Passwörter zu entwerfen. Dazu haben Sie die Empfehlungen, die ein großer Softwarekonzern diesbezüglich herausgegeben hat, wie folgt abgewandelt und konkretisiert:

| Schritt | Aktion | Empfehlung | Beispiel |
|---|---|---|---|
| 1 | Wähle zwei Sätze (mit insgesamt X Wörtern) | Denke an etwas Bedeutsames | Lange komplexe Passwörter sind die sichersten. Ich halte meins geheim. |
| 2 | Bilde aus den Sätzen eine Folge von Kleinbuchstaben | Benutze die jeweils ersten Buchstaben | lkpsdsihmg |
| 3 | Erhöhe die Komplexität | Ersetze alle Buchstaben der ersten oder der zweiten Hälfte des Alphabets durch Großbuchstaben | LKpsDsIHMG |
| 4 | Erhöhe die Wortlänge durch Ziffern | Füge jeweils eine Ziffer mit Bedeutung in die beiden Satzbereiche ein, wobei auch Satzanfang und -ende möglich sind. | LK1psDsIH2MG |
| 5 | Erhöhe die Wortlänge durch Interpunktionszeichen | Füge eines der 6 Symbole ! , . : ; ? zwischen den beiden Sätzen oder am Anfang oder am Ende des Wortes ein | LK1psDs?IH2MG |
| 6 | Erhöhe die Wortlänge durch spezielle Symbole | Füge eines der 22 Symbole # $ % & ( ) * + - / < = > @ [ \ ] ^ _ { \| } am Anfang oder am Ende ein | @LK1psDs?IH2MG |

Wie viele verschiedene Passwörter folgender Längen gibt es, wenn wir vereinfachend annehmen, dass alle Folgen von Kleinbuchstaben durch zwei Sätze erzeugt werden können (wobei wir die Umlaute ä, ö, ü ausschließen wollen) und Einwortsätze natürlich auch möglich sind:

(a) 8

(b) 10

(c) 12

(d) 14

(e) 16

**Lösung:** Durch Schritt 4 werden zwei Zeichen hinzugefügt, durch die Schritte 5 und 6 jeweils ein Zeichen. Daher entsteht ein Passwort der Länge $n$ aus $m = n - 4$ Wörtern.

Wir betrachten die Schritte einzeln:

- Schritte 1 und 2: Hier gibt es $26^m = 26^{n-4}$ Möglichkeiten, wenn wir ein zulässiges Alphabet der Kardinalität 26 annehmen.
- Schritt 3: 2 Möglichkeiten (erste oder zweite Hälfte).
- Schritt 4: Es gibt für die Wahl der ersten und der zweiten Ziffer jeweils 10 Möglichkeiten. Bei $m$ Wörtern kann die erste Ziffer an $m+1$ Stellen eingefügt werden; die zweite Ziffer kann dann an $m$ Stellen eingefügt werden. Da die Reihenfolge des Einfügens keine Rolle spielt, kompensieren wir die Doppelzählung per Division durch $2! = 2$. Für den Fall, dass die erste Ziffer am Ende des ersten Satzes und die zweite Ziffer am Anfang des zweiten Satzes eingefügt wird, sind die Ziffern benachbart, was in den obigen $(m+1)\cdot$

$m$ Möglichkeiten noch nicht berücksichtigt ist; hierdurch kommen noch einmal $m-1$ Möglichkeiten hinzu, insgesamt also

$$10^2 \cdot \left(\frac{1}{2} \cdot (m+1) \cdot m + (m-1)\right) = 100 \cdot \frac{1}{2} \cdot (n^2 - 5n + 2)$$

Möglichkeiten.

- Schritt 5: Hier wird eines von sechs Zeichen an einer von $m+1$ möglichen Stellen eingefügt.
- Schritt 6: Hier wird eines von 22 möglichen Zeichen an einer von zwei möglichen Stellen eingefügt.

Insgesamt erhalten wir also in Abhängigkeit der Passwortlänge $n$

$$W(n) = \underbrace{26^{n-4}}_{(1),(2)} \cdot \underbrace{2}_{(3)} \cdot \underbrace{100 \cdot \frac{1}{2} \cdot (n^2 - 5n + 2)}_{(4)} \cdot \underbrace{(n-3) \cdot 6}_{(5)} \cdot \underbrace{2 \cdot 22}_{(6)}$$

Möglichkeiten. Dies bedeutet für die konkret angegebenen Passwortlängen:

(a) W(8) = 1 568 341 632 000

(b) W(10) = 2 968 557 041 049 600

(c) W(12) = 4 267 088 706 720 153 600

(d) W(14) = 5 247 350 345 950 769 971 200

(e) W(16) = 5 829 716 790 879 499 458 969 600