ITET | Diskrete Mathematik | WS 02/03
R. Suter

Musterlösung Serie 4

1. a)

$$\begin{aligned} & 1\cdot 3+2\cdot 5+3\cdot 4+4\cdot 0+5\cdot 5+6\cdot 0+7\cdot 6+8\cdot a_8+9\cdot 9+10\cdot 2 \\ = \;& 3-1+1+0+3+0-2-3\,a_8+4-2 \mod 11 \\ = \;& 6-3a_8 \mod 11 \end{aligned}$$

Zu lösen ist: $6 = 3a_8 \mod 11$. — Lösung: $a_8 = 2$.

Die ISBN lautet 3–540–50629–2.

b) **1. Fall:** $\boxed{p > 5}$

Behauptung *Jede der Zahlen* $\underbrace{111...1}_{(p-1)\cdot k \text{ Stellen}}$ *mit* $k \in \mathbb{Z}_{>0}$ *ist durch* p *teilbar.*

Beweis Da p nicht 3 ist, ist die Teilbarkeit von 111...1 durch p äquivalent zur Teilbarkeit von 999...9 ($= 3^2 \cdot 111...1$) durch p.
Wegen $999...9 = 10^{\text{Anzahl Ziffern}} - 1$ muss man nur noch beweisen, dass

$$10^{(p-1)\cdot k} = 1 \mod p \qquad (\text{für } k \in \mathbb{Z}_{>0})$$

Dies folgt aus dem Kleinen Satz von Fermat:

$$\begin{aligned} 10^{p-1} &= 1 \mod p \qquad (\text{da } 10 \neq 0 \mod p) \\ \Rightarrow \qquad 10^{(p-1)\cdot k} &= \left(10^{p-1}\right)^k = 1 \mod p \end{aligned}$$

□

2. Fall: $\boxed{p = 3}$

Behauptung *Jede der Zahlen* $\underbrace{111...1}_{3k \text{ Stellen}}$ *mit* $k \in \mathbb{Z}_{>0}$ *ist durch* 3 *teilbar.*

Beweis $10 = 1 \mod 3$, also $10^\ell = 1 \mod 3$ für alle $\ell \in \mathbb{Z}_{>0}$:

$$111...1 = \sum_{\ell=0}^{(\text{Anzahl Stellen})-1} 10^\ell = \sum_{\ell}^{...} 1 = (\text{Anzahl Stellen}) \mod 3$$

Die Zahl ist durch 3 teilbar, sobald die Anzahl der Stellen durch 3 teilbar ist. □

Bitte wenden!

c) Zuerst einmal hat das Polynom $x^4 + 1$, wie die folgende Tabelle zeigt, keine Wurzeln in $\mathbb{F}_{11}$:

x	x^2	x^4	x^4+1	mod 11
0	0	0	1	
± 1	1	1	2	
± 2	4	5	-5	
± 3	-2	4	5	
± 4	5	3	4	
± 5	3	-2	-1	(alle $\neq 0$)

Deshalb können keine Linearfaktoren $(x - x_0)$ von $x^4 + 1$ abgespalten werden, und die einzige Möglichkeit, wie x^4+1 in ein Produkt von Polynomen aufspalten kann, wäre als Produkt von zwei quadratischen Polynomen:

$$x^4 + 1 = (x^2 + ax + b)(x^2 + Ax + B) \qquad \text{mit} \quad a, b, A, B \in \mathbb{F}_{11} \tag{1}$$

Entweder dies ist der Fall, die beiden Faktoren sind in diesem Fall irreduzibel (weil nicht weiter in Linearfaktoren zerlegbar), oder $x^4 + 1$ selbst ist nicht aufspaltbar.

Versuchen wir deshalb jetzt, (1) zu lösen:

$$\begin{aligned} x^4 + 1 &= (x^2 + ax + b)(x^2 + Ax + B) \\ \Longleftrightarrow \quad x^4 + 1 &= x^4 + (a + A)x^3 + (b + B + aA)x^2 + (aB + bA)x + bB\,. \end{aligned}$$

Koeffizientenvergleich ergibt (alles in $\mathbb{F}_{11}$, d. h. modulo 11):

$$\begin{aligned} a + A &= 0 \\ b + B + aA &= 0 \\ aB + bA &= 0 \\ bB &= 1 \end{aligned}$$

Die erste Gleichung sagt $\boxed{A = -a}$. — Die anderen sind damit äquivalent zu:

$$\begin{aligned} b + B - a^2 &= 0 \\ aB - ba &= 0 \\ bB &= 1 \end{aligned}$$

Die mittlere der drei Gleichungen kann auch als $a(B - b) = 0$ geschrieben werden und ergibt entweder $a = 0$ oder $B = b$.

Siehe nächstes Blatt!

1. Fall: $a = 0$

Die erste der drei Gleichungen gibt $B = -b$, und eingesetzt in die dritte Gleichung folgt:

$$-b^2 = 1 \mod 11$$

Wie man aus der oben stehenden Tabelle entnehmen kann, ist diese Gleichung $b^2 = -1$ nicht lösbar in $\mathbb{F}_{11}$. In diesem Fall ergibt sich also keine Lösung.

2. Fall: $\boxed{B = b}$

Die beiden restlichen zu lösenden Gleichungen lauten jetzt

$$a^2 = 2b \qquad \text{und} \qquad b^2 = 1$$

Die zweite Gleichung hat zwei Lösungen, $b = 1$ und $b = -1$; allerdings hat für $b = 1$ die andere Gleichung $a^2 = 2 \cdot 1$ keine Lösung (siehe Tabelle). Also muss $\boxed{b = -1}$ sein und $a^2 = -2$, d. h. $\boxed{a = \pm 3}$.

$$x^4 + 1 = (x^2 - 3x - 1)(x^2 + 3x - 1)$$

2. a) Links steht die Anzahl der k-elementigen Teilmengen einer Menge M aus $m + n$ Elementen.

Teile die ursprüngliche Menge M in zwei (disjunkte) Teilmengen X und Y auf mit $|X| = m$ und $|Y| = n$. Die Anzahl k-Teilmengen von M mit j Elementen aus X für $0 \leq j \leq k$ beträgt $\binom{m}{j}\binom{n}{k-j}$.

Summieren über j von 0 bis k ergibt die Vandermondesche Identität.

b) Benutzt die Vandermonde–Identität mit $m = k = n$:

$$\sum_{i=0}^{n} \binom{n}{i}^2 = \sum_{i=0}^{n} \binom{n}{i}\binom{n}{n-i} = \binom{2n}{n}$$

3. a) Wir behandeln gleich den allgemeinen Fall:

Es gibt so viele Monome $x_1^{a_1} x_2^{a_2} \cdot \ldots \cdot x_n^{a_n}$ in $(x_1 + \ldots + x_n)^d$ wie es Aufspaltungen der Zahl d als Summe

$$d = a_1 + \ldots + a_n$$

nichtnegativer ganzer Zahlen $a_1, \ldots, a_n$ gibt.

Dies ist die gleiche Zahl wie die Anzahl der Möglichkeiten, d Kugeln (●), durch $(n-1)$ Wände (|) voneinander in n Gruppen zu teilen, wobei auch „leere“ Gruppen zugelassen sind:

Bitte wenden!

Beispiel (für $d = 3$, $n = 3$ — 10 Möglichkeiten):

●●●|| |●●●| ||●●● ●●|●| ●|●●| ●●||● ●||●● |●●|● |●|●● ●|●|●

Hierbei gibt es $d + (n-1)$ Positionen für Kugeln und Wände, und wenn man daraus die $(n-1)$ Positionen ausgewählt/festgelegt hat, an denen die Wände stehen, sind auch die Positionen der Kugeln eindeutig bestimmt.

Für diese Auswahl gibt es

$$\binom{d + (n-1)}{n-1} \text{ Möglichkeiten}$$

(und damit auch $\binom{d+(n-1)}{n-1}$ verschiedene Monome $x_1^{a_1} \cdot \ldots \cdot x_n^{a_n}$ in $(x_1 + \ldots + x_n)^d$).

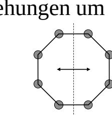
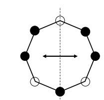
Im Fall $n = 3$ ergeben sich $\binom{d+2}{2}$ verschiedene Monome $x^a y^b z^c$ in $(x + y + z)^d$. Insbesondere erhält man bei $n = 3$, $d = 3$ wie im Beispiel der Aufgabe $\binom{5}{2} = 10$ als Ergebnis

b) Im Ganzen muss man n mal nach oben und m mal nach rechts gehen, also total $(n + m)$ Schritte, davon n nach oben. Jetzt kann man auswählen, wann man die n Schritte nach oben machen möchte, was dasselbe ist wie n aus $(n + m)$ auszuwählen.
Dafür gibt es $\binom{m+n}{n}$ Möglichkeiten.

4. Die Symmetriegruppe G des regelmässigen Achtecks besteht aus 16 Elementen: der Identität, Drehungen um den Winkel $\frac{360°}{8} \cdot d$ mit $d = \pm 1, \pm 2, \pm 3$ und 4 und jeweils 4 Spiegelungen an Achsen durch gegenübeliegende Eckpunkte bzw. gegenüberliegende Seitenmittelpunkte des Achtecks.

Für jedes Element g der Symmetriegruppe gilt es, die Anzahl der der Aufgabe entsprechenden Färbungen X^g auszurechnen, die invariant unter g sind.

a)

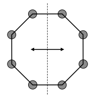
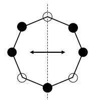
g	$\lvert X^g \rvert$	insgesamt
Identität	$\binom{8}{3} = \frac{8 \cdot 7 \cdot 6}{3 \cdot 2 \cdot 1} = 56$	56
Drehungen um $\frac{360°}{8} \cdot d$	0	$\times 7 = 0$
	0	$\times 4 = 0$
	$\binom{2}{1} \cdot \binom{3}{1} = 6$	$\times 4 = 24$
		$56 + 24 = 80$

Siehe nächstes Blatt!

Insgesamt gibt es nach Frobenius–Burnside–Lemma

$$\frac{1}{|G|}\sum_{g\in G}|X^g| = \frac{80}{16} = 5 \text{ Färbungen.}$$

b)

g	$\lvert X^g\rvert$	insgesamt
Identität	$2^8-2=254$	254
Drehungen um $\pm 45°$ bzw. $\pm 135°$	$2-2=0$	$\times 4 = 0$
Drehungen um $\pm 90°$	$2^2-2=2$	$\times 2 = 4$
Drehungen um $180°$	$2^4-2=14$	14
	$2^4-2=14$	$\times 4 = 56$
	$2^5-2=30$	$\times 4 = 120$
		$254+4+14+56+120=448$

(Die -2 in jeder Zeile stammt daher, dass wir jeweils die zwei Färbungen, für die sämtliche acht Ecken die gleiche Farbe haben, abziehen.)

Insgesamt gibt es nach Frobenius–Burnside–Lemma

$$\frac{1}{|G|}\sum_{g\in G}|X^g| = \frac{448}{16} = 28 \text{ Färbungen.}$$

Bemerkung: Von diesen 28 Färbungen bestehen

- jeweils eine aus einer mit der ersten Farbe und 7 mit der zweiten Farbe gefärbten Ecken;
- jeweils 4 aus 2 mit der ersten Farbe und 6 mit der zweiten Farbe gefärbten Ecken;
- jeweils 5 aus 2 mit der ersten Farbe und 6 mit der zweiten Farbe gefärbten Ecken (siehe oben);
- jeweils 8 aus gleichvielen Ecken der ersten Farbe wie der zweiten Farbe.

5. a) Bezeichne

- L die Menge aller Lehrer der Schule,
- A die Menge der Lehrer, die Klavier spielen,
- B die Menge der Lehrer, die Geige spielen und
- C die Menge der Lehrer, die Waldhorn spielen.

Bitte wenden!

Wäre die Behauptung wahr, dass 15% der Lehrer alle drei Instrumente spielen, würde sich aus dem Exklusions–Inklusions–Prinzip ergeben:

$$\begin{aligned} |A\cup B\cup C| &= |A|+|B|+|C|-|A\cap B|-|A\cap C|-|B\cap C|+|A\cap B\cap C| \\ &= 0,70\,|L|+0,60\,|L|+0,50\,|L| \\ &\quad -0,30\,|L|-0,40\,|L|-0,20\,|L|+0,15\,|L| \\ &= 1,05\,|L|\,, \end{aligned}$$

was nicht sein kann wegen $|A\cup B\cup C|\le |L|$.

Bemerkung: Aus den Angaben folgt übrigens noch mehr, nämlich, dass genau 10% der Lehrer alle drei Instrumente spielen.

b) Es **genügt zu zeigen**, dass es ein Paar a_i, a_j gibt mit $i \neq j$, so dass eine der Zahlen ein Vielfaches der anderen ist. Da die Zahlen a_k der Grösse nach geordnet sind, muss dann die Zahl mit dem kleineren Index wie behauptet die Zahl mit dem grösseren teilen.

Wir zerlegen jede der Zahlen a_k in ein Produkt

$$a_k = 2^{n_k} b_k$$

aus einer Zweierpotenz 2^{n_k} $(n_k \ge 0)$ und einer ungeraden Zahl b_k.

Dann **genügt es** jetzt zu zeigen, dass zwei der Zahlen b_i und b_j gleich sind; dann sind die zugehörigen a_i und a_j, wie gefordert, Vielfache voneinander.

Da die a_k Zahlen aus der Menge $\{1,2,\dots,2n\}$ sind, müssen die b_k ungerade Zahlen aus der Menge $\{1,2,\dots,2n\}$ sein. In dieser Menge liegen aber nur **n** ungerade Zahlen $(2\cdot 1-1, 2\cdot 3-1,\dots,2\cdot n-1)$, weshalb nach dem *Schubfachprinzip* zwei der $(\mathbf{n+1})$ Zahlen $b_1,\dots,b_{n+1}$ gleich sein müssen, und wir sind fertig. □

c) Betrachte die Mengen

$$\begin{aligned} S &= \{z\in\mathbb{N} \mid z \le 1'000'000 \text{ und } z\neq x^2,\ z\neq x^3,\ z\neq x^5 \text{ für alle } x\in\mathbb{N}\}\,, \\ B_2 &= \{z\in\mathbb{N} \mid z \le 1'000'000,\ z = x^2 \text{ für ein } x\in\mathbb{N}\}\,, \\ B_3 &= \{z\in\mathbb{N} \mid z \le 1'000'000,\ z = x^3 \text{ für ein } x\in\mathbb{N}\}\,, \\ B_5 &= \{z\in\mathbb{N} \mid z \le 1'000'000,\ z = x^5 \text{ für ein } x\in\mathbb{N}\}\,. \end{aligned}$$

Es gilt, die Menge

$$S = \{0,1,2,\dots,1'000'000\} - (B_2\cup B_3\cup B_5)$$

abzuzählen. Um das Inklusions–Exklusions–Prinzip anzuwenden, muss man sich Mengen der folgenden Art anschauen:

$$B_2\cap B_3 = \{z\in\mathbb{N} \mid z\le 1'000'000, z = x^6 \text{ für alle } x\in\mathbb{N}\}\,.$$

Siehe nächstes Blatt!

Diese Beschreibung ergibt sich aus der Eindeutigkeit der Zerlegung in Primfaktoren: $z \in B_2$ besagt, dass die Primfaktoren von x in Paaren auftreten, $z \in B_3$ sagt, dass die Primfaktoren von x in Tripeln auftreten. Stimmen die Zerlegungen überein, so müssen die Faktoren in 6-Tupeln auftreten. Analog:

$$\begin{aligned}
B_2 \cap B_5 &= \{ z \in \mathbb{N} \mid z \le 1'000'000,\ z = x^{10} \text{ für ein } x \in \mathbb{N} \}, \\
B_3 \cap B_5 &= \{ z \in \mathbb{N} \mid z \le 1'000'000,\ z = x^{15} \text{ für ein } x \in \mathbb{N} \}, \\
B_2 \cap B_3 \cap B_5 &= \{ z \in \mathbb{N} \mid z \le 1'000'000,\ z = x^{30} \text{ für ein } x \in \mathbb{N} \}.
\end{aligned}$$

B_2, B_3, B_5 und deren Schnitte sind leicht abzuzählen:

$$\begin{gathered}
|B_2| = 1001,\ |B_3| = 101,\ |B_5| = 16, \\
|B_2 \cap B_3| = 11,\ |B_2 \cap B_5| = 4,\ |B_3 \cap B_5| = 3, \\
|B_2 \cap B_3 \cap B_5| = 2\,.
\end{gathered}$$

Also ist

$$|S| = 1'000'001 - 1'001 - 101 - 16 + 11 + 4 + 3 - 2 = 998'899.$$