# Lösung zur Vordiplomklausur A „Diskrete Strukturen“

Marc Ensenbach

7. September 2001

---

**Ankreuzteil**

---

**Aufgabe A1**

(1) Nein. Die gegebene Rekursionsformel ist die für die Stirlingzahlen zweiter Art.

(2) Ja. Die Stirlingzahl erster Art $s_{n,k}$ gibt die Anzahl der Permutationen in $S_n$ an, die aus $k$ ziffernfremden Zyklen bestehen. Summiert man für festes $n$ über alle möglichen $k$, so erhält man die Anzahl aller Permutationen in $S_n$, also $n!$.

(3) Ja. $s_{n,n-1}$ ist die Anzahl der Permutationen in $S_n$, die aus $n-1$ ziffernfremden Zyklen bestehen. Eine solche Permutation besteht aus $n-2$ Einerzyklen und einem Zweierzyklus, und die Permutation ist durch die Angabe des Zweierzyklus bereits eindeutig bestimmt. Da es bei Zweierzyklen nicht auf die Reihenfolge der Zahlen ankommt, entspricht das Problem der Auswahl von zweielementigen Teilmengen der $S_n$, womit es genau $\binom{n}{2}$ solche Zyklen gibt.

(4) 11. Mit der Rekursionsformel $s_{n,k} = s_{n-1,k-1} + (n-1)s_{n-1,k}$ für Stirlingzahlen erster Art erhält man $s_{4,2} = s_{3,1} + 3s_{3,2} = 2 + 3 \cdot 3 = 11$.

---

**Aufgabe A2**

(1) Ja. $1+x$ ist in $\mathbb{Q}[[X]]$ invertierbar, da der konstante Term von Null verschieden ist. Damit ist auch $\frac{x}{1+x} = x\frac{1}{1+x}$ als Produkt zweier Elemente aus $\mathbb{Q}[[X]]$ in $\mathbb{Q}[[X]]$.

(2) Nein. $x$ ist in $\mathbb{Q}[[X]]$ nicht invertierbar, da der konstante Term Null ist.

(3) Ja. $x^3A = x^3\sum_{j=0}^{\infty} a_jx^j = \sum_{j=0}^{\infty} a_jx^{j+3} = \sum_{i=3}^{\infty} a_{i-3}x^i$ mit der Indexverschiebung $j \mapsto i-3$.

(4) Nein. $(1+x)^2 = 1 + 2x + x^2 \neq 1 + x^2 = 1^2 + 1^2x^2$.

---

**Aufgabe A3**

(1) Nein. Die Elemente in $K[x]$ mit Grad 0 sind gerade die Einheiten, und Einheiten sind nach Definition nicht irreduzibel.

(2) Ja. Ein Polynom der Form $x+a$ kann nicht in zwei irreduzible Polynome zerlegt werden.

(3) Nein. $x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$ hat in $\mathbb{Z}_2$ keine Nullstelle, ist aber nach (4) nicht irreduzibel.

(4) Nein. $x^4 + x^2 + 1 = (x^2 + x + 1)^2$.

---

**Aufgabe A4**

(1) 16. Jedes Polynom $g \in \mathbb{Z}_2[x]$ kann mit Polynomdivision geschrieben werden als $g = fq + r$ mit $\operatorname{Grad} r < \operatorname{Grad} f$. Da $[g]_f = [fq + r]_f = [r]_f$ gilt, bilden die Polynome mit einem Grad kleiner $\operatorname{Grad} f$ ein Vertretersystem. Da es in $\mathbb{Z}_2[x]$ genau $2^{\operatorname{Grad} f}$ Polynome mit einem Grad kleiner $\operatorname{Grad} f$ gibt, existieren hier $2^{\operatorname{Grad}(x^4+1)} = 2^4 = 16$ Vertreterpolynome, womit $|R| = 16$ gilt.

(2) Nein. Nach Vorlesung ist $R = K[x]/fK[x]$ für einen Körper $K$ und ein Polynom $f$ genau

dann ein Körper, wenn $f$ über $K[x]$ irreduzibel ist. Da $x^4+1=(x+1)^4$ gilt, ist $f$ nicht irreduzibel, also ist $R$ kein Körper.
(3) Ja. Es gilt $[x^2+x+1]\cdot[x^3+x^2+1]_f=[x^5+x^4+x^2+x^4+x^3+x+x^3+x^2+1]_f=[x^5+x+1]_f$. Da $x^5+x+1=(x^4+1)x+1$ ist, gilt $[x^5+x+1]_f=[1]_f$, also ist $[x^2+x+1]_f$ das Inverse von $[x^3+x^2+1]$.
(4) 5. Da $f=x^4+1=(x+1)^4$ gilt, sind die Teiler von $f$ genau die $(x+1)^i$, $i=0;1;\ldots;4$.

---

**Aufgabe A5**
(1) Ja. Satz der Vorlesung.
(2) Nein. Dann wäre die Summe der Grade $7\cdot 3=21$, was nicht möglich ist, da nach dem Handschlaglemma die Summe der Grade immer gerade ist.
(3) 15. Nach Vorlesung hat der vollständige Graph $\binom{6}{2}=\frac{1}{2}\cdot 6\cdot 5=15$ Kanten.

---

## Rechenaufgaben ohne Begründung

---

**Aufgabe R1**
(1) 60. Nach Vorlesung ist $|\operatorname{Inj}(\{1;2;3\};\{1;2;3;4;5\})|=|\{1;2;3;4;5\}|^{\underline{|\{1;2;3\}|}}=5^{\underline{3}}=5\cdot4\cdot3=60$.
(2) 14. Vorlesung: $|\operatorname{Surj}(\{1;2;3;4\};\{1;2\})|=|\{1;2\}|!\cdot S_{|\{1;2;3;4\}|,|\{1;2\}|}=2!S_{4,2}=2\cdot 7=14$.

---

**Aufgabe R2**
(1) Die Zykeldarstellung ist klarerweise $(1\ 7\ 2)(4\ 8\ 5\ 9\ 6)$.
(2) 12. Die Ordnung ist das positive kgV der einzelnen Zykellängen, sofern die Zykeln ziffernfremd sind, hier also $12\in \operatorname{kgV}(3;4)$.
(3) Die Darstellung lautet $(1\ 6\ 4)(2\ 5\ 7\ 3)$.
(4) Die Darstellung ist $(2\ 5\ 7\ 3)$, da $b^{27}=b^{2\cdot 12+3}=\left(b^{12}\right)^2 b^3=b^3$.

---

**Aufgabe R3**
$d=1$, $a=x$, $b=x^2+x+1$. Nach dem Euklidischen Algorithmus ist $x^4+1=(x^3+x^2+1)(x+1)+(x^2+x)$, $x^3+x^2+1=(x^2+x)x+1$, $x^2+x=1\cdot(x^2+x)$, also ist 1 ein ggT von $x^4+1$ und $x^3+x^2+1$. Durch Rückwärtsauflösen erhält man $1=(x^3+x^2+1)-(x^2+x)x=(x^3+x^2+1)-((x^4+1)-(x^3+x^2+1)(x+1))x=g-(f-(x+1)g)x=g-(xf-(x^2+x)g)=(x^2+x+1)g-xf=(x^2+x+1)g+xf$.

---

**Aufgabe R4**
(1) 40. $\varphi(100)=\varphi(2^2\cdot 5^2)=\varphi(2^2)\cdot\varphi(5^2)=(2-1)\cdot 2\cdot(5-1)\cdot 5=2\cdot 4\cdot 5=40$.
(2) 69. Nach dem Satz von Euler ist $a^{\varphi(m)}\equiv 1 \mod m$ für $1\in \operatorname{ggT}(a;m)$. Da $1\in\operatorname{ggT}(13;100)$ ist, gilt $13^{162}=13^{40\cdot 4+2}=\left(13^{\varphi(100)}\right)^4\cdot 13^2\equiv 13^2=169\equiv 69 \mod 100$.

---

**Aufgabe R5**
(1) 4. Es gilt immer $\dim C=l-\operatorname{Grad} g$, ($l$ Codelänge), hier $\dim C=7-3=4$.
(2) 16. $C$ ist ein $\mathbb{Z}_2$-Vektorraum der Dimension 4, hat also $|\mathbb{Z}_2|^4=2^4=16$ Elemente.
(3) 3. Nach einem Beispiel aus der Vorlesung ist die Minimaldistanz größer/gleich 3, und da der zu 1 gehörige Codierungsvektor $(1;1;0;1;0;0;0)$, erhalten über die 7-Bit-Darstellung von $1\cdot g$, vom Nullvektor die Distanz 3 hat, muß 3 auch die Minimaldistanz sein.
(4) 1. Da $(1;1;0;0;0;0;0)$ zu $(1;1;0;1;0;0;0)$ die Distanz 1 hat, wird der gegebene Vektor zu $(1;1;0;1;0;0;0)$ korrigiert. Nach (3) liefert die Decodierung dieses Vektors 1.

---

**Aufgabe R6**
$\{2;4;5\}$. Rekonstruiert man den Baum aus dem Prüfercode, so erhält man der Reihe nach

die Kanten $\{1;2\}$; $\{4;3\}$; $\{5;3\}$; $\{3;2\}$; $\{2;6\}$. Daher ist 3 mit den Knoten 4, 5 und 2 verbunden.

---

## Aufgaben mit Lösungsweg

---

**Aufgabe L1**

Sei $A = \sum_{n=0}^{\infty} a_n x^n$. Dann gilt $A = a_0 + a_1 x + \sum_{n=2}^{\infty} a_n x^n$. Setzt man die Anfangsbedingungen und die Rekursionsformel ein, erhält man $A = 1 + x + \sum_{n=2}^{\infty}(a_{n-1} + 2a_{n-2})x^n = 1 + x + \sum_{n=2}^{\infty} a_{n-1}x^n + 2\sum_{n=2}^{\infty} a_{n-2}x^n = 1 + x + x\sum_{n=2}^{\infty} a_{n-1}x^{n-1} + 2x^2\sum_{n=2}^{\infty} a_{n-2}x^{n-2} = 1+x+x\sum_{n=1}^{\infty} a_n x^n + 2x^2\sum_{n=0}^{\infty} a_n x^n = 1+x+x\sum_{n=0}^{\infty} a_n x^n - x + 2x^2\sum_{n=0}^{\infty} a_n x^n = 1+xA+2x^2A$, durch Auflösen nach $A$ folgt $A = \frac{1}{1-x-2x^2}$. Das reflektierte Polynom des Nenners lautet $x^2-x-2$, es hat die Nullstellen $\beta = -1$ und $\gamma = 2$. Damit läßt sich $A$ darstellen als $\frac{1}{(1+x)(1-2x)}$.
Nun setzt man mit Partialbruchzerlegung an: $\frac{1}{(1+x)(1-2x)} = \frac{B}{1+x} + \frac{C}{1-2x} \Leftrightarrow 1 = (1-2x)B+(1+x)C = B-2xB+C+xC = (B+C)+x(C-2B)$. Durch Koeffizientenvergleich erhält man $B+C = 1 \wedge C-2B = 0 \quad \Leftrightarrow \quad C = 1-B \wedge 1-3B = 0 \quad \Leftrightarrow \quad B = \frac{1}{3} \wedge C = \frac{2}{3}$. Analog zum Beispiel der Fibonacci-Folge aus der Vorlesung erhält man $a_n = B\beta^n + C\gamma^n = \frac{1}{3}(-1)^n + \frac{2}{3}\cdot 2^n$.

---

**Aufgabe L2**

Um die gesuchten $n$ zu finden, bestimmt man diejenigen Primzahlpotenzen, deren $\varphi$-Funktionswert ein Teiler von 6 ist: $\varphi(p^m) = (p-1)p^{m-1} = 1 \Leftrightarrow p = 2 \wedge m = 1$, $\varphi(p^m) = 2 \Leftrightarrow (p-1 = 2 \wedge p^{m-1} = 1) \vee (p-1 = 1 \wedge p^{m-1} = 2) \Leftrightarrow (p = 3 \wedge m = 1) \vee (p = 2 \wedge m = 2)$, $\varphi(p^m) = 3 \Leftrightarrow (p-1 = 3 \wedge p^{m-1} = 1) \vee (p-1 = 1 \wedge p^{m-1} = 3)$, dieses Gleichungssystem hat keine Lösung, $\varphi(p^m) = 6 \Leftrightarrow (p-1 = 6 \wedge p^{m-1} = 1) \vee (p-1 = 3 \wedge p^{m-1} = 2) \vee (p-1 = 2 \wedge p^{m-1} = 3) \vee (p-1 = 1 \wedge p^{m-1} = 6) \Leftrightarrow (p = 7 \wedge m = 1) \vee (p = 3 \wedge m = 2)$, da die zweite und vierte Gleichung keine Lösungen haben.
Damit erhält man zunächst direkt $\varphi(7) = 6$ und $\varphi(9) = \varphi(3^2) = 6$, aus der Darstellung $6 = 6 \cdot 1$ erhält man $\varphi(14) = \varphi(7^1) \cdot \varphi(2^1) = 6 \cdot 1 = 6$ und $\varphi(18) = \varphi(3^2 \cdot 2) = \varphi(3^2) \cdot \varphi(2^1) = 6 \cdot 1 = 6$, aus den Darstellungen $6 = 3 \cdot 2$ und $6 = 3 \cdot 2 \cdot 1$ erhält man keine weitere Lösungen, da $\varphi(p^m)$ für Primzahlpotenzen $p^m$ niemals 3 werden kann, wie oben gezeigt wurde. Damit lauten die Zahlen $n$ mit $\varphi(n) = 6$: $7, 9, 14, 18$, die ungeraden Lösungen sind 7 und 9.
Durch Ausprobieren erhält man $\mathbb{Z}_7^* = \{[1]_7; [2]_7; [3]_7; [4]_7; [5]_7; [6]_7\} = \langle [3]_7 \rangle = \langle [5]_7 \rangle$ und $\mathbb{Z}_9^* = \{[1]_9; [2]_9; [4]_9; [5]_9; [7]_9; [8]_9\} = \langle [2]_9 \rangle = \langle [5]_9 \rangle = \langle [8]_9 \rangle$, also sind beide primen Restklassengruppen zyklisch, alle erzeugenden Elemente sind bereits angegeben.

---