

Mathematik I für Studierende der Informatik und Wirtschaftsinformatik (Diskrete Mathematik) im Wintersemester 2017/18

16. November 2017

Modulare Arithmetik

Definition 3.33

Es sei m eine natürliche Zahl. Zwei ganze Zahlen a und b sind *kongruent modulo m* , falls a und b denselben Rest bei Division durch m haben.

Ist a kongruent zu b modulo m , so schreiben wir $a \equiv b \pmod{m}$.
 $a \equiv b \pmod{m}$ gilt genau dann, wenn $a - b$ durch m teilbar ist.

Definition 3.36

Für jede natürliche Zahl m und jede ganze Zahl a heißt die Menge $[a]_m := \{b \in \mathbb{Z} : b \bmod m = a \bmod m\}$ die *Restklasse von a modulo m* .

Für jede natürliche Zahl m gibt es genau m verschiedene Restklassen modulo m , nämlich $[0]_m, \dots, [m-1]_m$.
Diese Restklassen sind paarweise disjunkt und es gilt $\mathbb{Z} = [0]_m \cup \dots \cup [m-1]_m$.

Satz 3.37

Für alle $m \in \mathbb{N}$ und alle $a, b, c, d \in \mathbb{Z}$ gilt:

1. $a \equiv a \pmod{m}$
2. $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$
3. $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$
4. $a \equiv b \pmod{m} \Rightarrow -a \equiv -b \pmod{m}$
5. $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$
6. Gilt $\text{ggT}(c, m) = 1$, so folgt aus $c \cdot a \equiv c \cdot b \pmod{m}$ die Kongruenz $a \equiv b \pmod{m}$.

Definition 3.39

Für eine reelle Zahl r ist $\lceil r \rceil$ die kleinste ganze Zahl $\geq r$.

Analog ist $\lfloor r \rfloor$ die größte ganze Zahl $\leq r$.

Man nennt $\lceil \quad \rceil$ die *obere Gaußklammer* und $\lfloor \quad \rfloor$ die *untere Gaußklammer*.

Für alle $m \in \mathbb{Z}$ und $n \in \mathbb{N}$ gilt $m \operatorname{div} n = \lfloor \frac{m}{n} \rfloor$ sowie
 $m \operatorname{mod} n = m - n \cdot \lfloor \frac{m}{n} \rfloor$.

Elementare Kombinatorik

Definition 4.1

Für eine endliche Menge M sei $|M|$ die Anzahl der Elemente von M .

Satz 4.2

1. (Additionsregel) M sei eine endliche Menge und M_1, \dots, M_n seien disjunkte Teilmengen von M mit $M = M_1 \cup \dots \cup M_n$. Dann gilt

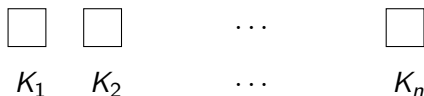
$$|M| = \sum_{i=1}^n |M_i|.$$

2. (Multiplikationsregel) Seien A_1, \dots, A_n endliche Mengen. Dann gilt

$$|A_1 \times \dots \times A_n| = |A_1| \cdot \dots \cdot |A_n| = \prod_{i=1}^n |A_i|.$$

3. (Gleichheitsregel) Seien A und B zwei endliche Mengen. Dann gilt $|A| = |B|$ genau dann, wenn es eine Bijektion $f : A \rightarrow B$ gibt.

Eine typische Anwendung der Multiplikationsregel ist die folgende:
Für ein $n \in \mathbb{N}$ betrachten wir n Kästchen K_1, \dots, K_n .



In das erste Kästchen K_1 legen wir ein Objekt a_1 , in das zweite Kästchen K_2 ein Objekt a_2 und so weiter.

Wenn wir k_1 Möglichkeiten haben, das erste Kästchen K_1 zu belegen, k_2 Möglichkeiten, das zweite Kästchen K_2 zu belegen und so weiter, dann gibt es insgesamt $k_1 \cdot k_2 \cdot \dots \cdot k_n$ Möglichkeiten, die n Kästchen zu belegen.

Beispiel 4.3

1. Eine Kennziffer bestehe aus drei Buchstaben und vier darauffolgenden Ziffern, wie *FAB3447* oder *ARR5510*. Wieviele derartige Kennziffern gibt es?

Nach der Multiplikationsregel gibt es

$$26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 \cdot 10 = 26^3 \cdot 10^4 = 175760000$$

Kennziffern.

2. Wieviele Kennziffern wie in (1) gibt es, in denen kein Buchstabe und keine Ziffer doppelt vorkommen?

Nach der Multiplikationsregeln ergibt sich

$$26 \cdot 25 \cdot 24 \cdot 10 \cdot 9 \cdot 8 \cdot 7 = 78624000.$$

3. Gegeben seien 15 unterschiedliche Bücher, von denen 8 auf Englisch, 3 auf Deutsch und 4 auf Russisch sind. Auf wie viele Arten kann man zwei Bücher in verschiedenen Sprachen auswählen?

Nach Additions- und Multiplikationsregel ergibt sich

$$8 \cdot 3 + 8 \cdot 4 + 3 \cdot 4 = 68.$$

Wir diskutieren im Folgenden fünf grundlegende Fragestellungen, die wir Grundaufgaben nennen.

Vorher definieren wir noch Tupel der Länge 0.

Definition 4.4

Für eine beliebige Menge M sei \emptyset das eindeutig bestimmte 0-Tupel von Elementen von M . Mit anderen Worten, $M^0 = \{\emptyset\}$.

Grundaufgabe 1. Es seien $n, k \in \mathbb{N}_0$. Wie viele k -Tupel von Elementen einer n -elementigen Menge gibt es?

Antwort: n^k

Diese Antwort ergibt sich sofort mit Hilfe der Multiplikationsregel.



Beispiel 4.5

1. Sei $M = \{a, b\}$. Dann gibt es $2^3 = 8$ 3-Tupel von Elementen von M .

Es gilt

$$M^3 = \{(a, a, a), (a, a, b), (a, b, a), (a, b, b), \\ (b, a, a), (b, a, b), (b, b, a), (b, b, b)\}.$$

2. Sei $M = \{a, b, c, d, e, f, g\}$. Dann gibt es $7^3 = 343$ 3-Tupel von Elementen von M .

Grundaufgabe 2. Es seien $n, k \in \mathbb{N}_0$. Wieviele k -Tupel von Elementen einer n -elementigen Menge gibt es, in denen kein Element doppelt vorkommt?

Antwort: Falls $k \geq 1$ ist, so gibt es nach der Multiplikationsregel $n \cdot (n - 1) \cdot \dots \cdot (n - (k - 1))$ k -Tupel von Elementen einer n -elementigen Mengen, in denen kein Element doppelt vorkommt. Ist $k = 0$, so gibt es genau ein k -Tupel. □

Definition 4.6

Für $n, k \in \mathbb{N}_0$ sei

$$n^{\underline{k}} := \begin{cases} n \cdot (n-1) \cdot \dots \cdot (n-k+1), & \text{falls } k \geq 1 \text{ und} \\ 1, & \text{sonst.} \end{cases}$$

Beispiel 4.7

1. $7^{\underline{0}} = 1$
2. $7^{\underline{1}} = 7$
3. $7^{\underline{2}} = 7 \cdot 6 = 42$
4. $7^{\underline{3}} = 7 \cdot 6 \cdot 5 = 210$

Beispiel 4.8

Sei $M = \{a, b, c, d, e, f, g\}$. Dann gibt es $7^3 = 210$ 3-Tupel von Elementen von M , in denen kein Element doppelt vorkommt.

Definition 4.9

Sei M eine Menge. Eine *Permutation* von M ist eine Bijektion $\pi : M \rightarrow M$.

Beispiel 4.10

Sei $M = \{1, 2, 3\}$. Wir definieren $\pi : M \rightarrow M$ durch $\pi(1) = 3$, $\pi(2) = 1$ und $\pi(3) = 2$. Dann ist π eine Permutation auf M .

Ist M eine endliche Menge $\{m_1, \dots, m_n\}$, wobei wir annehmen, dass die m_i paarweise verschieden sind, so kann man eine Permutation $\pi : M \rightarrow M$ in der Form

$$\begin{pmatrix} m_1 & m_2 & \dots & m_n \\ \pi(m_1) & \pi(m_2) & \dots & \pi(m_n) \end{pmatrix}$$

darstellen.

Aus der Grundaufgabe 2 ergibt sich, dass die Anzahl der Permutationen einer n -elementigen Menge genau

$$n^n = n \cdot (n - 1) \cdot \dots \cdot 1 \text{ ist.}$$

Anstelle von n^n schreibt man üblicher Weise $n!$ (gelesen “ n Fakultät”).

Beispiel 4.11

$$0! = 0^0 = 1, 1! = 1^1 = 1, 2! = 2^2 = 2 \cdot 1 = 2,$$
$$10! = 10^{10} = 10 \cdot 9 \cdot \dots \cdot 2 \cdot 1 = 3628800.$$

Beispiel 4.12

1. Sei $M = \{1, 2, 3\}$. Dann gibt es genau $3! = 3 \cdot 2 \cdot 1 = 6$ Permutationen von M :

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

2. Sei $M = \{a, b, c, d, e, f, g\}$. Dann gibt es $7! = 5040$ Permutationen von M .

Grundaufgabe 3. Es sei $n \geq k \geq 0$. Wieviele k -elementige Teilmengen einer n -elementigen Menge gibt es?

Antwort: Es gibt $\frac{n^k}{k!}$ k -elementige Teilmengen einer n -elementigen Menge.

Für die Anzahl der k -elementigen Teilmengen einer n -elementigen Menge schreibt man auch $\binom{n}{k}$.

Es gilt

$$\binom{n}{k} = \frac{n^k}{k!} = \frac{n^k \cdot (n-k)!}{k! \cdot (n-k)!} = \frac{n!}{k! \cdot (n-k)!}.$$

Ist $k \geq 1$, so können wir auch

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdot \dots \cdot (n-k+1)}{k \cdot (k-1) \cdot \dots \cdot 1}$$

schreiben.

Definition 4.13

Für $n, k \in \mathbb{N}_0$ mit $n \geq k \geq 0$ nennt man die Zahl $\binom{n}{k} = \frac{n^k}{k!}$ einen *Binomialkoeffizienten*.

Beispiel 4.14

Sei $M = \{a, b, c, d, e, f, g\}$. Dann hat M genau

$$\binom{7}{3} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2 \cdot 1} = 35$$

3-elementige Teilmengen.

Satz 4.15 (Rekursive Berechnung der Binomialkoeffizienten)

Für alle $n, k \in \mathbb{N}$ mit $n \geq 2$ und $1 \leq k \leq n - 1$ gilt

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Wir ordnen die Binomialkoeffizienten wie folgt im *Pascalschen Dreieck* an:

$$\begin{array}{ccccccc} & & & & \binom{0}{0} & & & & \\ & & & & \binom{1}{0} & & \binom{1}{1} & & \\ & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & \\ & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} \\ \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} \end{array}$$

Die Binomialkoeffizienten verdanken ihren Namen dem folgenden Satz:

Satz 4.16 (Binomischer Lehrsatz)

Seien $a, b \in \mathbb{R}$. Dann gilt für alle $n \in \mathbb{N}_0$

$$\begin{aligned}(a + b)^n &= \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i \\ &= a^n + \binom{n}{1} a^{n-1} b + \dots + \binom{n}{n-1} a b^{n-1} + b^n.\end{aligned}$$

Wir bemerken noch zwei wichtige Regeln für Binomialkoeffizienten.

Korollar 4.18

1. Für alle $n \in \mathbb{N}_0$ gilt $2^n = \sum_{i=0}^n \binom{n}{i}$.
2. Für alle $n, k \in \mathbb{N}_0$ mit $n \geq k$ gilt $\binom{n}{k} = \binom{n}{n-k}$.

Korollar 4.19

Sei $n \in \mathbb{N}_0$ und sei M eine n -elementige Menge. Dann hat $\mathcal{P}(M)$ genau 2^n Elemente.

Grundaufgabe 4. Sei $n \in \mathbb{N}$ und $k \in \mathbb{N}_0$. Es seien n Gefäße K_1, \dots, K_n gegeben, auf die k ununterscheidbare Kugeln verteilt werden sollen.

Wieviele Möglichkeiten gibt es, die Kugeln zu verteilen?

Antwort. Es gibt $\binom{n+k-1}{k}$ Möglichkeiten, die Kugeln zu verteilen.

Beispiel 4.20

Angenommen, k Abgeordnete wählen je einen von n Kandidaten. Keiner der Abgeordneten enthält sich. Dann gibt es $\binom{n+k-1}{k}$ mögliche Verteilungen der k Stimmen auf die n Kandidaten.

Grundaufgabe 5. Gegeben seien r verschiedene Zeichen Z_1, \dots, Z_r . Wie viele verschiedene Zeichenfolgen der Länge n kann man aus den Zeichen Z_1, \dots, Z_r bilden, wenn man verlangt, dass das Zeichen Z_1 genau n_1 -mal auftritt, das Zeichen Z_2 genau n_2 -mal und so weiter.

Beispiel 4.21

Wie viele Wörter lassen sich aus den Buchstaben des Wortes ANAGRAMM bilden (wobei alle Buchstaben verwendet werden sollen)?

Antwort zu Grundaufgabe 5. Es gibt genau

$$\frac{(n_1 + \dots + n_r)!}{n_1! \cdot \dots \cdot n_r!}$$

Zeichenfolgen aus den Zeichen Z_1, \dots, Z_r , in denen für jedes $i \in \{1, \dots, r\}$ das Zeichen Z_i genau n_i -mal vorkommt.

Definition 4.22

Seien $n_1, \dots, n_r \in \mathbb{N}_0$ und $n = \sum_{i=1}^r n_i$. Dann nennt man

$$\binom{n}{n_1, \dots, n_r} = \frac{n!}{n_1! \cdot \dots \cdot n_r!}$$

einen *Multinomialkoeffizienten*.

Im Spezialfall $r = 2$ sind die Multinomialkoeffizienten genau die schon betrachteten Binomialkoeffizienten.

Sei nämlich $n = n_1 + n_2$. Dann gilt

$$\begin{aligned} \binom{n}{n_1, n_2} &= \frac{n!}{n_1! \cdot n_2!} = \frac{n!}{n_1! \cdot (n - n_1)!} = \binom{n}{n_1} \\ &= \frac{n!}{n_2! \cdot (n - n_2)!} = \binom{n}{n_2}. \end{aligned}$$

Die ersten vier Grundaufgaben gehen alle auf dieselbe grundlegende Frage zurück: Wieviele Möglichkeiten gibt es, k Elemente aus einer n -elementigen Menge zu ziehen? Dabei wird auf unterschiedliche Weisen gezogen, und die Ergebnisse werden auf unterschiedliche Arten gezählt. Es gibt folgende Möglichkeiten:

1. Ziehen mit Zurücklegen, wobei die Reihenfolge, in der die Elemente gezogen werden, berücksichtigt wird.
2. Ziehen ohne Zurücklegen, mit Berücksichtigung der Reihenfolge.
3. Ziehen ohne Zurücklegen, ohne Berücksichtigung der Reihenfolge.
4. Ziehen mit Zurücklegen, ohne Berücksichtigung der Reihenfolge.

Satz 4.23

Seien $n, k \in \mathbb{N}_0$. Dann gibt es genau n^k Möglichkeiten, k Elemente mit Zurücklegen aus einer n -elementigen Menge zu ziehen, wobei die Reihenfolge, in der die Elemente gezogen werden, berücksichtigt wird.

Beweis.

Die Möglichkeiten, die k Elemente zu ziehen, entsprechen genau den k -Tupeln von Elementen der n -elementigen Menge. Gemäß der Lösung von Grundaufgabe 1 gibt es also genau n^k Möglichkeiten. □

Satz 4.24

Seien $n, k \in \mathbb{N}_0$ mit $k \leq n$. Dann gibt es genau n^k Möglichkeiten, k Elemente ohne Zurücklegen aus einer n -elementigen Menge zu ziehen, wobei die Reihenfolge, in der die Elemente gezogen werden, berücksichtigt wird.

Beweis.

Die Möglichkeiten, die k Elemente zu ziehen, entsprechen genau den k -Tupeln von Elementen der n -elementigen Menge, in denen kein Element doppelt vorkommt. Gemäß der Lösung von Grundaufgabe 2 gibt es also genau n^k Möglichkeiten. □

Satz 4.25

Seien $n, k \in \mathbb{N}_0$ mit $k \leq n$. Dann gibt es genau $\binom{n}{k}$ Möglichkeiten, k Elemente ohne Zurücklegen aus einer n -elementigen Menge zu ziehen, wobei die Reihenfolge, in der die Elemente gezogen werden, nicht berücksichtigt wird.

Beweis.

Die Möglichkeiten, die k Elemente zu ziehen, entsprechen genau den k -elementigen Teilmengen der n -elementigen Menge. Gemäß der Lösung von Grundaufgabe 3 gibt es also genau $\binom{n}{k}$ Möglichkeiten. □

Satz 4.26

Seien $n, k \in \mathbb{N}_0$. Dann gibt es genau $\binom{n+k-1}{k}$ Möglichkeiten, k Elemente mit Zurücklegen aus einer n -elementigen Menge zu ziehen, wobei die Reihenfolge, in der die Elemente gezogen werden, nicht berücksichtigt wird.

Satz 4.27 (Multinomialsatz)

Seien $r, n \in \mathbb{N}_0$. Dann gilt für alle $x_1, \dots, x_r \in \mathbb{R}$

$$(x_1 + \dots + x_r)^n = \sum_{n_1 + \dots + n_r = n} \binom{n}{n_1, \dots, n_r} x_1^{n_1} \cdot \dots \cdot x_r^{n_r}.$$

Diese Summe läuft über alle r -Tupel $(n_1, \dots, n_r) \in \mathbb{N}_0^r$ mit $n_1 + \dots + n_r = n$.

Man beachte, dass man für $r = 2$ aus dem Multinomialsatz genau den Binomialsatz erhält.