

Sächsisches Landesseminar Mathematik 2024 in Sayda

11.03. – 15.03.2024

Begleitmaterial zum Seminarprogramm der Klassenstufe 10

Herausgegeben im Auftrag des Sächsischen Landeskomitees zur Förderung
mathematisch-naturwissenschaftlich begabter und interessierter Schüler

Vorwort

Liebe Schülerinnen,
liebe Schüler,

ich freue mich, Euch im Sächsischen Landesseminar Mathematik begrüßen zu können.

In den nächsten drei Tagen werdet Ihr zehn mathematische Seminare haben. Ich hoffe, dass Ihr während dieser Seminare nicht nur neue Lösungsmethoden oder mathematische Sachverhalte kennen lernt, sondern dass Ihr dabei auch Freude an der Mathematik und am Lösen von Aufgaben haben werdet.

Am Donnerstag wird dann die Auswahlklausur geschrieben, für die ich Euch jetzt schon alles Gute und viel Erfolg wünsche. Während Ihr am vorbereiteten Freizeitprogramm teilnehmt, werden die Klausuren korrigiert. Am Freitag wird dann die Mannschaft, die Sachsen auf der Bundesrunde der Mathematik-Olympiade vertreten darf, feierlich bekannt gegeben.

Ich hoffe, dass Ihr es in den nächsten Tagen neben der Mathematik auch genießen könnt, Euch mit Gleichgesinnten zu unterhalten, Euch auszutauschen und um Lösungsansätze gemeinsam zu ringen. Dazu soll insbesondere auch der MatBoj beitragen. Aber natürlich denke ich dabei auch an die vielen Spiele, die eine lange Tradition im Landesseminar haben.

Ich wünsche Euch viel Erfolg und eine gute Woche.

Joachim Lippert

Über dieses Heft

Dieses Heft behandelt einige der wichtigsten Themen für die Mathematik-Olympiade in der Klassenstufe 10. Einige dieser Themen werden auch in den Seminaren besprochen, einige werdet ihr bestimmt schon kennen und andere werden euch neu sein. Es wird empfohlen, dass ihr das Heft zur Vorbereitung auf die Bundesrunde oder die nächste Olympiade durcharbeitet.

In diesem Heft gibt es zwei Typen von Aufgaben: *Beispielaufgaben* und *Übungsaufgaben*. An Beispielaufgaben lassen sich die vorgestellten Methoden besonders gut vorführen. Manchmal lösen wir Beispielaufgaben direkt auf, aber meistens findet ihr am Ende des jeweiligen Kapitels Tipps und erst ganz am Ende des Heftes die Lösungen für die Beispielaufgaben. Die Beispielaufgaben solltet ihr zuerst bearbeiten, wenn ihr euch mit einer neuen Methode vertraut machen wollt. Bei den Übungsaufgaben hingegen seid ihr auf euch allein gestellt. Sie dienen zur weiteren Vertiefung der Inhalte.

Schwere Aufgaben sind mit einem (*) bis drei (***) Sternen gekennzeichnet. Ein Stern bedeutet dabei, dass die Aufgabe schwerer als die durchschnittliche Bundesrunden-Aufgabe ist. Besonders bei solchen Aufgaben gilt: Wenn ihr nicht weiterkommt, dann holt euch einen Tipp und wenn ihr dann immer noch feststeckt, dann lest euch auch gern die Lösung durch – dafür sind die Tipps und die Lösungen schließlich da.

Texte: Ferdinand Wagner. Mit tatkräftiger Unterstützung von Sebastian Bürger, Leo Gitin, Cara Hobohm, Tien Nguyen und Arne Wolf. Aufbauend auf früheren Texten von Ingolf Busch, Frank Göhring, Maximilian Keitel, Eric Müller, Jens Reinhold und Lisa Sauermann. Herzlichen Dank auch an alle weiteren, die in früheren Ausgaben dieses Begleitheftes Beiträge erstellt haben.

Textsatz: Joachim Lippert, Tien Nguyen, Ferdinand Wagner.

Redaktion: Joachim Lippert (lippert@landesseminar-sachsen.de).

Inhaltsverzeichnis

Gleichungen und Ungleichungen	4
1 Lineare Rekursionen	4
2 Die Schuirhead-Ungleichung	9
3 Die Ungleichungen von Jensen und Karamata	15
Geometrie	18
4 Potenzgeraden	18
5 (Dreh-)Streckungen	22
6 Geometrieaufgaben durchrechnen	29
Kombinatorik	37
7 Der Heiratssatz	37
Zahlentheorie	40
8 Multiplikative Ordnungen und Primitivwurzeln	40
9 Quadratische Reste	45
Lösungen zu den Beispielaufgaben	50
MatBoj-Regeln	63

1 Lineare Rekursionen

In der Mathe-Olympiade begegnen euch regelmäßig Rekursionsgleichungen. Zum Teil sind sie direkt Teil der Aufgabe, zum Teil treten sie erst in eurer Lösung auf. In diesem Kapitel lernt ihr, wie ihr Rekursionsgleichungen von einem spezifischen Typ in explizite Formeln umwandeln könnt. Das wird euch in einigen Aufgaben eine große Hilfe sein.

Mehr zu Rekursionen findet ihr in Kapitel 1: *Lineare Rekursionen*.

Fibonacci-Zahlen

Bevor wir das allgemeine Verfahren erläutern, werden wir zum Warmwerden eine explizite Formel für die Fibonacci-Zahlen herleiten. An diesem Beispiel lässt sich die Methode hervorragend demonstrieren und der allgemeine Fall wird uns danach leicht fallen.

Wir erinnern uns, dass die *Fibonacci-Folge* $(F_n)_{n \geq 0}$ durch die Anfangsbedingungen $F_0 = 0, F_1 = 1$ und die Rekursionsgleichung $F_{n+2} = F_{n+1} + F_n$ für alle $n \geq 0$ gegeben ist. Wir fragen uns zuerst, ob eine reelle Zahl λ existiert, sodass die Zahlenfolge $(\lambda^n)_{n \geq 0}$ die gleiche Rekursionsgleichung wie die Fibonacci-Folge erfüllt (wir behaupten allerdings *nicht*, dass die Fibonacci-Folge selber von dieser Form sein muss). Dann müsste also

$$\lambda^{n+2} = \lambda^{n+1} + \lambda^n$$

für alle $n \geq 0$ erfüllt sein. Wenn wir $\lambda \neq 0$ annehmen (was eine vernünftige Annahme ist, sonst würden wir ja einfach die Nullfolge bekommen), dann sind diese Gleichungen äquivalent zu $\lambda^2 = \lambda + 1$. Mit der üblichen Lösungsformel für quadratische Gleichungen erhalten wir, dass die Lösungen dieser Gleichung durch den *goldenen Schnitt* und sein *Konjugiertes*

$$\phi := \frac{1 + \sqrt{5}}{2} \quad \text{und} \quad \bar{\phi} := \frac{1 - \sqrt{5}}{2}.$$

gegeben sind. Folglich erfüllen die Zahlenfolgen $(\phi^n)_{n \geq 0}$ und $(\bar{\phi}^n)_{n \geq 0}$ die gleiche Rekursion wie die Fibonacci-Zahlen. Für beliebige reelle Zahlen α und β erfüllt dann auch $(\alpha\phi^n + \beta\bar{\phi}^n)_{n \geq 0}$ die gleiche Rekursion. Wenn wir α und β so wählen, dass das Gleichungssystem

$$\begin{cases} \alpha\phi^0 + \beta\bar{\phi}^0 = 0, \\ \alpha\phi^1 + \beta\bar{\phi}^1 = 1 \end{cases}$$

erfüllt ist, dann stimmen die Zahlenfolgen $(F_n)_{n \geq 0}$ und $(\alpha\phi^n + \beta\bar{\phi}^n)_{n \geq 0}$ an den Stellen $n = 0$ und $n = 1$ überein und außerdem erfüllen sie die gleiche Rekursionsgleichung. Folglich müssen sie überall übereinstimmen! Wir müssen also nur noch das Gleichungssystem lösen! Aus der ersten Gleichung folgt $\alpha = -\beta$. In die zweite Gleichung eingesetzt liefert das $\alpha = 1/(\phi - \bar{\phi}) = 1/\sqrt{5}$ und somit $\beta = -1/\sqrt{5}$. Insgesamt haben wir das folgende Resultat bewiesen:

Formel von Binet. Die Fibonacci-Folge $(F_n)_{n \geq 0}$ besitzt die folgende explizite Darstellung:

$$F_n = \frac{1}{\sqrt{5}} (\phi^n - \bar{\phi}^n).$$

Das allgemeine Verfahren

Wir betrachten nun das allgemeine Problem. Angenommen, wir haben eine Zahlenfolge $(a_n)_{n \geq 0}$, deren Werte („Anfangsbedingungen“) a_0, a_1, \dots, a_{k-1} bekannt sind. Ferner soll $(a_n)_{n \geq 0}$ die Rekursionsgleichung

$$a_{n+k} = c_{k-1}a_{n+k-1} + \dots + c_1a_{n+1} + c_0a_n$$

erfüllen, wobei c_0, c_1, \dots, c_{k-1} vorgegebene reelle Zahlen sind. Um zu einer expliziten Formel zu gelangen, wollen wir die Überlegungen aus dem vorherigen Unterabschnitt verallgemeinern und gelangen zu dem folgenden Verfahren:

- (a) Wir suchen zunächst nach Zahlen λ , sodass die Zahlenfolge $(\lambda^n)_{n \geq 0}$ die gleiche Rekursionsgleichung erfüllt. Das führt auf die sogenannte charakteristische Gleichung

$$\lambda^k = c_{k-1}\lambda^{k-1} + \dots + c_1\lambda + c_0.$$

Üblicherweise hat diese Gleichung k Lösungen $\lambda = \lambda_1, \lambda_2, \dots, \lambda_k$. Wir erhalten also k Folgen $(\lambda_i^n)_{n \geq 0}$, $i = 1, 2, \dots, k$, die die gegebene Rekursion erfüllen.

- (b) Also erfüllt auch jede Folge der Form $(\alpha_1\lambda_1^n + \alpha_2\lambda_2^n + \dots + \alpha_k\lambda_k^n)_{n \geq 0}$ diese Rekursion. Wir wollen nun $\alpha_1, \alpha_2, \dots, \alpha_k$ so wählen, dass auch die Anfangswerte stimmen. Dafür stellen wir das folgende Gleichungssystem auf:

$$\begin{cases} \alpha_1\lambda_1^0 + \alpha_2\lambda_2^0 + \dots + \alpha_k\lambda_k^0 = a_0 \\ \alpha_1\lambda_1^1 + \alpha_2\lambda_2^1 + \dots + \alpha_k\lambda_k^1 = a_1 \\ \vdots \\ \alpha_1\lambda_1^{k-1} + \alpha_2\lambda_2^{k-1} + \dots + \alpha_k\lambda_k^{k-1} = a_{k-1} \end{cases}$$

Wenn sich das Gleichungssystem lösen lässt, dann ist

$$a_n = \alpha_1\lambda_1^n + \alpha_2\lambda_2^n + \dots + \alpha_k\lambda_k^n \quad \text{für alle } n \geq 0.$$

Das Verfahren funktioniert, weil die beiden Folgen $(a_n)_{n \geq 0}$ und $(\alpha_1\lambda_1^n + \alpha_2\lambda_2^n + \dots + \alpha_k\lambda_k^n)_{n \geq 0}$ in ihren k Anfangswerten übereinstimmen und die gleiche Rekursion erfüllen, sodass sie überall gleich sein müssen. Damit liefert das Verfahren eine explizite Darstellung für a_n .

Allerdings kann das Verfahren immer noch schiefgehen:

Problem 1. In Schritt (a) suchen wir die Lösungen der charakteristischen Gleichung, bzw. äquivalent die Nullstellen des *charakteristischen Polynoms*

$$\chi(\lambda) := \lambda^k - (c_{k-1}\lambda^{k-1} + \dots + c_1\lambda + c_0).$$

Nun kann es passieren, dass $\chi(\lambda)$ keine reellen Nullstellen hat. Zum Beispiel führt die Rekursion $a_{n+2} = -a_n$ auf die charakteristische Gleichung $\lambda^2 = -1$ bzw. das charakteristische Polynom $\chi(\lambda) = \lambda^2 + 1$. Es hindert uns aber niemand, die Nullstellen in den *komplexen Zahlen* zu suchen (siehe Kapitel 6: *Geometrie-Aufgaben durchrechnen*). Es lässt sich zeigen, dass jedes Polynom vom Grad k über den komplexen Zahlen in k Linearfaktoren zerfällt.¹ Wir finden also stets komplexe Zahlen $\lambda_1, \lambda_2, \dots, \lambda_k$, sodass

$$\chi(\lambda) = (\lambda - \lambda_1)(\lambda - \lambda_2) \cdots (\lambda - \lambda_k).$$

Damit stellt Problem 1 kein wirkliches Problem dar.

Problem 2. In Schritt (b) lösen wir ein Gleichungssystem. Es kann passieren, dass dieses Gleichungssystem keine Lösungen hat.

Dieser Fall kann eintreten, wenn $\chi(\lambda)$ eine *Doppelnulstelle* hat, also wenn mindestens zwei der Nullstellen $\lambda_1, \lambda_2, \dots, \lambda_k$ gleich sind. Denn dann können wir in $\alpha_1\lambda_1^n + \alpha_2\lambda_2^n + \dots + \alpha_k\lambda_k^n$ nicht mehr k freie Parameter $\alpha_1, \alpha_2, \dots, \alpha_k$ wählen, wodurch das Gleichungssystem in (b)

¹Dieses Resultat ist als *Fundamentalsatz der Algebra* bekannt, obwohl es in Wirklichkeit eher ein Resultat aus der komplexen Analysis ist.

überbestimmt ist: Es hat mehr Gleichungen als freie Parameter. Solche Gleichungssysteme sind im Allgemeinen nicht lösbar. Im nächsten Abschnitt werden wir ein konkretes Beispiel sehen und erklären, wie sich das Problem beheben lässt.

Wenn $\chi(\lambda)$ keine Doppelnullstellen hat, also wenn $\lambda_1, \lambda_2, \dots, \lambda_k$ paarweise verschieden sind, dann lässt sich das Gleichungssystem aus (b) stets eindeutig lösen. Der einfachste Beweis dafür benutzt allerdings Matrizen und Determinanten, was ihr wahrscheinlich noch nicht kennt.² Aber zum Lösen einer *konkreten* Rekursion müsst ihr den allgemeinen Beweis natürlich nicht kennen, sondern lediglich feststellen, dass sich euer Gleichungssystem in dem konkreten Fall lösen lässt.

Was passiert bei Doppelnullstellen?

Wir werden wieder zuerst an einem Beispiel erklären, wie sich das Problem mit Doppelnullstellen beheben lässt. Betrachte dazu die Folge $(a_n)_{n \geq 0}$ mit $a_0 = 1$, $a_1 = 1$ und $a_{n+2} = 4a_{n+1} - 4a_n$. In diesem Fall ist $\chi(\lambda) = \lambda^2 - 4\lambda + 4 = (\lambda - 2)^2$. Wir erhalten also die Nullstellen 2 und 2 und damit zweimal die Folge $(2^n)_{n \geq 0}$. Das entstehende Gleichungssystem

$$\begin{cases} \alpha \cdot 2^0 + \beta \cdot 2^0 = 1, \\ \alpha \cdot 2^1 + \beta \cdot 2^1 = 1 \end{cases}$$

hat keine Lösung. Aus der ersten Gleichung folgt nämlich $\alpha + \beta = 1$, während die zweite Gleichung $\alpha + \beta = \frac{1}{2}$ liefert. Nun fällt uns aber auf, dass auch die Zahlenfolge $(n2^{n-1})_{n \geq 0}$ die Rekursionsgleichung erfüllt, denn $(n+2)2^{n+1} = 4 \cdot (n+1)2^n - 4 \cdot n2^{n-1}$. Wir können also versuchen, geeignete Koeffizienten α und β mit $a_n = \alpha \cdot 2^n + \beta \cdot n2^{n-1}$ zu finden. Das führt auf das folgende Gleichungssystem:

$$\begin{cases} \alpha \cdot 2^0 + \beta \cdot 0 \cdot 2^{-1} = 1, \\ \alpha \cdot 2^1 + \beta \cdot 1 \cdot 2^0 = 1. \end{cases}$$

Dieses Gleichungssystem hat die eindeutige Lösung $\alpha = 1$, $\beta = -1$. Wir erhalten also die explizite Darstellung $a_n = 2^n - n2^{n-1}$.

Betrachten wir nun den allgemeinen Fall, dass das charakteristische Polynom $\chi(\lambda)$ eine s -fache Nullstelle bei $\lambda = \lambda_i$ hat. Dann erfüllen die Folgen

$$(n(n-1) \cdots (n-r+1) \lambda_i^{n-r})_{n \geq 0} \quad \text{für } r = 0, 1, \dots, s-1$$

ebenfalls die gegebene Rekursionsgleichung. Ein besonders eleganter Beweis hierfür benutzt Ableitungen³, aber es lässt sich auch mit Methoden der Klasse 10 zeigen und sei euch als Übungsaufgabe überlassen.

²Der Beweis geht folgendermaßen: Wir schreiben die Koeffizienten des Gleichungssystems in eine $n \times n$ -Matrix (also eine Tabelle). Um zu zeigen, dass das Gleichungssystem eine eindeutige Lösung hat, müssen wir zeigen, dass die Determinante dieser Matrix $\neq 0$ ist. Die Matrix hat eine spezielle Form, die als *Vandermonde-Matrix* bekannt ist. Nach der *Vandermonde-Formel* gilt

$$\det \begin{pmatrix} \lambda_1^0 & \lambda_2^0 & \cdots & \lambda_k^0 \\ \lambda_1^1 & \lambda_2^1 & \cdots & \lambda_k^1 \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{k-1} & \lambda_2^{k-1} & \cdots & \lambda_k^{k-1} \end{pmatrix} = \prod_{1 \leq i < j \leq k} (\lambda_j - \lambda_i).$$

Wenn $\lambda_1, \lambda_2, \dots, \lambda_k$ paarweise verschieden sind, ist das Produkt auf der rechten Seite offensichtlich $\neq 0$, wie gewünscht.

³Es ist nämlich kein Zufall, dass die Formel $n(n-1) \cdots (n-r+1) \lambda_i^{n-r}$ wie eine r -te Ableitung aussieht: Wenn $\chi(\lambda)$ eine s -fache Nullstelle bei $\lambda = \lambda_i$ hat, dann hat auch $\lambda^n \chi(\lambda)$ eine s -fache Nullstelle bei $\lambda = \lambda_i$. Für alle $r = 0, 1, \dots, s-1$ folgt, dass die r -te Ableitung der Funktion $\lambda^n \chi(\lambda)$ ebenfalls eine Nullstelle bei $\lambda = \lambda_i$ hat. Wenn ihr aufschreibt, wie die r -te Ableitung von $\lambda^n \chi(\lambda)$ aussieht und was es bedeutet, dass sie bei $\lambda = \lambda_i$ eine Nullstelle hat, erhaltet ihr genau, dass $(n(n-1) \cdots (n-r+1) \lambda_i^{n-r})_{n \geq 0}$ die gegebene Rekursionsgleichung erfüllt.

Mit dieser Beobachtung können wir unser ursprüngliches Verfahren so modifizieren, dass es immer funktioniert:

- (a') Bestimme die komplexen Nullstellen $\lambda_1, \lambda_2, \dots, \lambda_l$ des charakteristischen Polynoms $\chi(\lambda)$, wobei λ_i mit Vielfachheit s_i auftritt. Dann gilt $s_1 + s_2 + \dots + s_l = k$ und die Folgen

$$(n(n-1)\cdots(n-r_i+1)\lambda_i^{n-r_i})_{n \geq 0} \quad \text{für } i = 1, 2, \dots, l \text{ und } r_i = 0, 1, \dots, s_i - 1$$

liefern k verschiedene Lösungen der Rekursionsgleichung.

- (b') Also erfüllt auch jede Folge der Form

$$\sum_{i=1}^l \sum_{r_i=0}^{s_i-1} \alpha_{i,r_i} n(n-1)\cdots(n-r_i+1)\lambda_i^{n-r_i}$$

die Rekursion. Wir wollen die Koeffizienten α_{i,r_i} so wählen, dass die Anfangswerte genau a_0, a_1, \dots, a_{k-1} sind. Analog zu (b) führt das auf ein Gleichungssystem mit k Gleichungen und k Variablen.

Es lässt sich (wiederum mit Determinanten⁴) zeigen, dass das Gleichungssystem aus (b') stets eine eindeutige Lösung hat. Damit haben wir ein allgemeines Verfahren, mit dem sich tatsächlich jede lineare Rekursion in eine explizite Darstellung umwandeln lässt.

Inhomogene lineare Rekursionen

Eine *inhomogene lineare Rekursion* ist eine Rekursionsgleichung der Form

$$b_{n+k} = c_{k-1}b_{n+k-1} + \dots + c_1b_{n+1} + c_0b_n + f(n),$$

wobei $f: \mathbb{Z}_{\geq 0} \rightarrow \mathbb{R}$ eine vorgegebene Funktion ist. Gesucht ist wieder eine explizite Formel für die Folge $(b_n)_{n \geq 0}$, die durch die obige Rekursion und vorgegebene Anfangswerte b_0, b_1, \dots, b_{k-1} gegeben ist. Bisher haben wir nur *homogene lineare Rekursionen* betrachtet, also solche, für die $f(n) = 0$ für alle $n \geq 0$ gilt.

Als erstes fällt uns auf: Wenn $(b_n)_{n \geq 0}$ und $(\bar{b}_n)_{n \geq 0}$ die obige inhomogene Rekursionsgleichung erfüllen, dann erfüllt $(\bar{b}_n - b_n)_{n \geq 0}$ die entsprechende homogene Rekursion (also die gleiche Rekursionsgleichung bloß ohne $f(n)$). Folglich müssen wir bloß *eine* Lösung der inhomogenen Rekursionsgleichung finden und können dann alle anderen Lösungen konstruieren, indem wir eine Lösung der homogenen Rekursion addieren. Insbesondere können wir die Anfangswerte b_0, b_1, \dots, b_{k-1} zunächst ignorieren und dann durch Addition einer geeigneten Lösung der homogenen Gleichung korrigieren.

Im Allgemeinen ist es jedoch alles andere als einfach, überhaupt nur *eine* Lösung der inhomogenen Rekursionsgleichung zu finden. Wir werden im Folgenden beschreiben, wie das für einen Spezialfall funktioniert, nämlich den Fall $f(n) = P(n)C^n$, wobei $P(n)$ ein Polynom in n und C eine Konstante ist. Damit lässt sich schon eine große Familie von Fällen abdecken. Denn wenn $f(n) = f_1(n) + f_2(n)$ die Summe zweier Funktionen ist, dann genügt es, eine Lösung für $f_1(n)$

⁴Wir erklären die Idee im Fall, dass $\lambda_1 = \lambda_2$ eine Doppelnullstelle ist. Der allgemeine Fall geht völlig analog. Betrachte zuerst eine Vandermonde-Matrix wie oben, wobei $\lambda_2 = \lambda_1 + h$. Wenn wir die erste Spalte von der zweiten Spalte subtrahieren, ändert sich die Determinante bekanntlich nicht. Wenn wir danach die zweite Spalte durch h dividieren, wird auch die Determinante durch h dividiert. Im Limes $h \rightarrow 0$ wird die zweite Spalte zur „Ableitung“ der ersten Spalte, also erhalten wir genau die gewünschte Matrix! Das Produkt $\prod_{i < j} (\lambda_j - \lambda_i)$ enthält den Faktor $\lambda_2 - \lambda_1 = h$, der gekürzt wird, wenn wir durch h teilen. Alle anderen Faktoren $\lambda_j - \lambda_2 = \lambda_j - (\lambda_1 + h)$ für $2 < j$ werden im Limes $h \rightarrow 0$ zu $\lambda_j - \lambda_1 \neq 0$. Also erhalten wir immer noch ein Produkt, das nicht 0 sein kann.

und eine Lösung für $f_2(n)$ zu finden und diese Lösungen zu addieren. Wir bekommen also nicht nur den Fall $f(n) = P(n)C^n$, sondern auch beliebige Summen von Termen dieser Form. Das deckt die allermeisten Fälle ab, die euch in der Mathe-Olympiade begegnen werden.

Bevor wir den kompletten Spezialfall $f(n) = P(n)C^n$ betrachten, gehen wir durch einige Spezialfälle des Spezialfalls.

Fall 1: $f(n) = c$ ist eine Konstante. In diesem Fall gibt es einen einfachen Trick: Wir subtrahieren die Rekursionsgleichung für n von der Gleichung für $n + 1$ und erhalten

$$b_{n+k+1} - b_{n+k} = c_{k-1}(b_{n+k} - b_{n+k-1}) + \cdots + c_1(b_{n+2} - b_{n+1}) + c_0(b_{n+1} - b_n).$$

Das ist nun eine homogene Rekursionsgleichung. Ferner fällt uns auf: Wenn $\chi(\lambda)$ das charakteristische Polynom der ursprünglichen Rekursion ist, dann ist das charakteristische Polynom der neuen Gleichung genau $(\lambda - 1)\chi(\lambda)$. Wenn wir die Nullstellen von $\chi(\lambda)$ kennen, dann kennen wir also auch die Nullstellen des neuen charakteristischen Polynoms und wir können die Methode aus den vorherigen Abschnitten anwenden.

Fall 2: $f(n) = P(n)$ ist ein Polynom in n . Wir wenden den gleichen Trick wie in Fall 1 mehrfach an. Wenn wir die Rekursionsgleichung für n von der Gleichung für $n + 1$ subtrahieren, erhalten wir eine inhomogene Rekursionsgleichung mit $f(n) = P(n+1) - P(n)$. Wenn $P(n)$ ein Polynom vom Grad d ist, dann ist $P(n+1) - P(n)$ ein Polynom vom Grad $d - 1$. Indem wir die neue Gleichung für $n + 1$ von der neuen Gleichung für n subtrahieren, erhalten wir ein Polynom vom Grad $d - 2$ und so weiter. Nach $d + 1$ Schritten ist $f(n)$ ein Polynom vom Grad -1 , also $f(n) = 0$ und wir haben eine homogene Rekursionsgleichung. In jedem Schritt wird das charakteristische Polynom mit $\lambda - 1$ multipliziert, also erhalten wir am Ende das charakteristische Polynom $(\lambda - 1)^{d+1}\chi(\lambda)$. Hierauf können wir die Methode aus den vorherigen Abschnitten anwenden.

Fall 3: $f(n) = C^n$ für eine reelle Zahl C . In diesem Fall nehmen wir die Rekursionsgleichung für n , multiplizieren sie mit C und subtrahieren sie dann von der Gleichung für $n + 1$. Wir erhalten

$$b_{n+k+1} - Cb_{n+k} = c_{k-1}(b_{n+k} - Cb_{n+k-1}) + \cdots + c_1(b_{n+2} - Cb_{n+1}) + c_0(b_{n+1} - Cb_n).$$

Das ist nun eine homogene Rekursionsgleichung und das charakteristische Polynom der neuen Gleichung ist genau $(\lambda - C)\chi(\lambda)$. Wir können also wiederum die Methode aus den vorherigen Abschnitten anwenden.

Allgemeiner Fall. Wir kombinieren die Ideen aus Fall 2 und Fall 3, um den Fall $f(n) = P(n)C^n$ zu lösen, wobei $P(n)$ ein Polynom vom Grad d in n und C eine Konstante ist. Wir nehmen wieder die Rekursionsgleichung für n , multiplizieren sie mit C und subtrahieren sie von der Gleichung für $n + 1$. Das ganze wiederholen wir $d + 1$ mal. Im i -ten Schritt erhalten wir eine inhomogene Rekursionsgleichung mit $f(n) = P_i(n)C^n$, wobei $P_0(n) = P(n)$ und $P_i(n) = P_{i-1}(n+1) - P_{i-1}(n)$. Per Induktion folgt, dass $P_i(n)$ ein Polynom vom Grad $d - i$ ist. Insbesondere ist $P_i(n) = 0$ für $i \geq d + 1$. Folglich erhalten wir nach $d + 1$ Schritten eine homogene Rekursionsgleichung. In jedem Schritt wird das charakteristische Polynom mit $\lambda - C$ multipliziert, also erhalten wir am Ende das charakteristische Polynom $(\lambda - C)^{d+1}\chi(\lambda)$. Hierauf können wir die Methode aus den vorherigen Abschnitten anwenden. Damit sind wir fertig!

2 Die Schuirhead-Ungleichung

Was könnt ihr tun, wenn ihr bei einer Ungleichung nicht weiterkommt? *Brute force!* Ihr könnt brutal mit allen Nennern durchmultiplizieren, so lange quadrieren, bis alle Wurzeln weg sind, und am Ende werdet ihr einen riesigen Haufen Terme übrig haben, die ihr irgendwie gegeneinander abschätzen müsst.

In so einer Situation ist die *Schuirhead-Ungleichung* hilfreich. Hinter diesem (nicht ganz ernst gemeinten) Namen verbergen sich in Wirklichkeit zwei Ungleichungen: nämlich die *Muirhead-* und die *Schur-Ungleichung*. In diesem Kapitel werdet ihr beide kennenlernen.

Die Muirhead-Ungleichung

In diesem Abschnitt benutzen wir die folgende Notation: Sei $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ ein n -Tupel von nichtnegativen reellen Zahlen und seien x_1, x_2, \dots, x_n Variablen. Dann schreiben wir

$$T_\alpha(x_1, x_2, \dots, x_n) := \sum_{\sigma \in \mathfrak{S}_n} x_1^{\alpha_{\sigma(1)}} x_2^{\alpha_{\sigma(2)}} \cdots x_n^{\alpha_{\sigma(n)}}.$$

Hier bezeichnet \mathfrak{S}_n die Menge aller Permutationen von $\{1, 2, \dots, n\}$, die Summe erstreckt sich somit über alle $n!$ Vertauschungen der Exponenten $\alpha_1, \alpha_2, \dots, \alpha_n$. Es gilt also zum Beispiel $T_{(2,1,0)}(x, y, z) = x^2y + xy^2 + y^2z + yz^2 + z^2x + xz^2$ und $T_{(1,1,1)}(x, y, z) = 6xyz$.

Definition. Seien $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ und $\beta = (\beta_1, \beta_2, \dots, \beta_n)$ zwei n -Tupel von nichtnegativen reellen Zahlen. Wir sagen α *majorisiert* β und schreiben $\alpha \succcurlyeq \beta$, wenn gilt:

$$\begin{aligned} \alpha_1 &\geq \beta_1 \\ \alpha_1 + \alpha_2 &\geq \beta_1 + \beta_2 \\ &\vdots \\ \alpha_1 + \alpha_2 + \cdots + \alpha_{n-1} &\geq \beta_1 + \beta_2 + \cdots + \beta_{n-1} \\ \alpha_1 + \alpha_2 + \cdots + \alpha_n &= \beta_1 + \beta_2 + \cdots + \beta_n. \end{aligned}$$

Beachte, dass in der letzten Zeile (und nur dort) eine Gleichheit steht!

Zum Beispiel gilt $(2, 1, 0) \succcurlyeq (1, 1, 1)$. Allgemein gilt: Wenn $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$ absteigend geordnete nichtnegative reelle Zahlen sind, dann gilt

$$(\alpha_1, \alpha_2, \dots, \alpha_n) \succcurlyeq \left(\frac{\alpha_1 + \alpha_2 + \cdots + \alpha_n}{n}, \frac{\alpha_1 + \alpha_2 + \cdots + \alpha_n}{n}, \dots, \frac{\alpha_1 + \alpha_2 + \cdots + \alpha_n}{n} \right).$$

Es kann aber auch vorkommen, dass weder $\alpha \succcurlyeq \beta$ noch $\beta \succcurlyeq \alpha$ gilt. Das ist zum Beispiel immer der Fall, wenn $\alpha_1 + \alpha_2 + \cdots + \alpha_n \neq \beta_1 + \beta_2 + \cdots + \beta_n$. Aber es gibt auch nichttriviale Gegenbeispiele wie etwa $\alpha = (\frac{3}{2}, \frac{3}{2}, 0)$ und $\beta = (\frac{5}{3}, 1, \frac{1}{3})$.

Muirhead-Ungleichung. Gegeben seien absteigend geordnete n -Tupel $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$, $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n \geq 0$ und $\beta = (\beta_1, \beta_2, \dots, \beta_n)$, $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_n \geq 0$. Wenn $\alpha \succcurlyeq \beta$, dann gilt für alle $x_1, x_2, \dots, x_n \geq 0$ die folgende Ungleichung:

$$T_\alpha(x_1, x_2, \dots, x_n) \geq T_\beta(x_1, x_2, \dots, x_n).$$

Wenn alle x_i positiv sind, dann tritt Gleichheit genau für $x_1 = x_2 = \cdots = x_n$ oder $\alpha = \beta$ ein.

Wegen $(1, 0, 0, \dots, 0) \succcurlyeq (\frac{1}{n}, \frac{1}{n}, \dots, \frac{1}{n})$ ist die AM-GM-Ungleichung ein Spezialfall der Muirhead-Ungleichung. Umgekehrt lässt sich die Muirhead-Ungleichung mit der gewichteten AM-GM-Ungleichung beweisen. Insofern könnt ihr jede Aufgabe, die sich mit der Muirhead-Ungleichung

erschlagen lässt, auch mit gewichtetem AM-GM beweisen. Trotzdem ist die Muirhead-Ungleichung nützlich zu wissen, weil sie euch ein wichtiges Kriterium liefert, wann ihr eine Aufgabe mit gewichtetem AM-GM lösen könnt. Zudem spart ihr euch ein wenig Zeit in der Olympiade, wenn ihr nicht erst die richtigen Gewichte herausfinden müsst.

Der Beweis der Muirhead-Ungleichung ist ziemlich technisch, aber wir besprechen ihn trotzdem (unter anderem, weil ulkigerweise der Heiratssatz verwendet wird; siehe Kapitel 7: *Der Heiratssatz*). Wenn ihr keine Lust darauf habt, dann überspringt ihn ruhig, ihr verpasst nichts.

Wir benötigen zuerst ein ziemlich technisches Lemma.

Majorisierungs-Lemma. *Seien α und β zwei absteigend geordnete n -Tupel von nichtnegativen reellen Zahlen, sodass $\alpha \succ \beta$. Dann gibt es nichtnegative reelle Zahlen $\mu_\sigma \geq 0$, $\sigma \in \mathfrak{S}_n$, mit*

$$\sum_{\sigma \in \mathfrak{S}_n} \mu_\sigma = 1 \quad \text{und} \quad \beta_i = \sum_{\sigma \in \mathfrak{S}_n} \mu_\sigma \alpha_{\sigma(i)} \quad \text{für alle } i = 1, \dots, n.$$

Ihr könnt euch das Majorisierungs-Lemma anschaulich so erklären, dass es uns eine mögliche Wahl von Gewichten liefert, die wir brauchen, um die Muirhead-Ungleichung aus der gewichteten AM-GM-Ungleichung herzuleiten.

Beweis. Der Beweis besteht aus zwei Schritten. Wir werden zuerst beide Schritte vorstellen, danach beweisen wir sie.

- (1) *Es gibt nichtnegative reelle Zahlen $\lambda_{i,j} \geq 0$, $i, j = 1, 2, \dots, n$, die die folgenden Bedingungen erfüllen:*

$$\sum_{i=1}^n \lambda_{i,j} = 1 \quad \text{für alle } j, \quad \sum_{j=1}^n \lambda_{i,j} = 1 \quad \text{für alle } i, \quad \beta_i = \sum_{j=1}^n \lambda_{i,j} \alpha_j \quad \text{für alle } i.$$

Um diese Behauptung besser zu verstehen, betrachten wir die *Matrix* $\Lambda = (\lambda_{i,j})$. Λ ist nichts weiteres als eine $n \times n$ -Tabelle mit dem Eintrag $\lambda_{i,j}$ an der (i, j) -ten Stelle. Die ersten beiden Bedingungen sagen dann bloß, dass die Summe der Einträge in jeder Spalte und jeder Zeile genau 1 ist.⁵

Um den zweiten Schritt zu formulieren, müssen wir etwas Notation einführen. Für zwei Matrizen $A = (a_{i,j})$ und $B = (b_{i,j})$ schreiben wir $A + B := (a_{i,j} + b_{i,j})$ für die Matrix, in der wir die entsprechenden Einträge von A und B addiert haben. Wenn μ eine reelle Zahl ist, schreiben wir $\mu A := (\mu a_{i,j})$ für die Matrix, in der wir jeden Eintrag von A mit μ multipliziert haben. Außerdem ist eine *Permutationsmatrix* eine Matrix, in der in jeder Spalte und jeder Zeile genau ein Eintrag 1 ist und alle anderen Einträge 0 (sozusagen ein „ $n \times n$ -Sudoku mit 0 und 1“). Für jede Permutation $\sigma \in \mathfrak{S}_n$ erhalten wir eine Permutationsmatrix P_σ , in der der (i, j) -te Eintrag 1 ist, falls $\sigma(i) = j$, und sonst 0. Umgekehrt ist jede Permutationsmatrix von der Form P_σ für ein $\sigma \in \mathfrak{S}_n$.

Der zweite Schritte besagt nun:

- (2) *Sei $\Lambda = (\lambda_{i,j})$ eine Matrix mit nichtnegativen reellen Einträgen, in der die Summe der Einträge in jeder Zeile und jeder Spalte 1 ist. Dann gibt es nichtnegative reelle Zahlen $\mu_\sigma \geq 0$, $\sigma \in \mathfrak{S}_n$, mit*

$$\sum_{\sigma \in \mathfrak{S}_n} \mu_\sigma = 1 \quad \text{und} \quad \Lambda = \sum_{\sigma \in \mathfrak{S}_n} \mu_\sigma P_\sigma$$

⁵Wenn ihr schon einmal mit Matrizen gearbeitet habt, werdet ihr außerdem erkennen, dass die dritte Bedingung genau $\Lambda \cdot \alpha = \beta$ aussagt, wobei wir α und β als Spaltenvektoren auffassen. Aber ihr könnt den Beweis auch verstehen, wenn ihr das Produkt von Matrizen und Vektoren noch nicht kennt.

Aus (1) und (2) folgt die Aussage des Majorisierungslemmas sofort. Wir müssen also nur diese beiden Behauptungen beweisen.

Beweis von (1). Für zwei absteigend geordnete n -Tupel α und β schreiben wir $\alpha \succcurlyeq' \beta$, wenn die Bedingung aus (1) erfüllt ist. Wir bemerken zuerst: Wenn $\gamma = (\gamma_1, \gamma_2, \dots, \gamma_n)$ ein weiteres n -Tupel von nichtnegativen reellen Zahlen ist, dann folgt aus $\alpha \succcurlyeq' \gamma$ und $\gamma \succcurlyeq' \beta$ schon $\alpha \succcurlyeq' \beta$. Denn wenn $\gamma_i = \sum_{j=1}^n \lambda'_{i,j} \alpha_j$ und $\beta_i = \sum_{j=1}^n \lambda''_{i,j} \gamma_j$, dann können wir die Ausdrücke für γ_j in den Ausdruck für β_i einsetzen und erhalten eine Darstellung $\beta_i = \sum_{j=1}^n \lambda_{i,j} \alpha_j$ mit $\lambda_{i,j} = \sum_{k=1}^n \lambda'_{i,k} \lambda''_{k,j}$, die die gewünschten Bedingungen erfüllt.⁶

Um (1) zu beweisen, werden wir eine Folge $\alpha = \gamma^{(0)}, \gamma^{(1)}, \dots, \gamma^{(n)} = \beta$ konstruieren, sodass sowohl $\gamma^{(0)} \succcurlyeq \gamma^{(1)} \succcurlyeq \dots \succcurlyeq \gamma^{(n)}$ als auch $\gamma^{(0)} \succcurlyeq' \gamma^{(1)} \succcurlyeq' \dots \succcurlyeq' \gamma^{(n)}$ gilt und sodass jedes $\gamma^{(i)}$ mindestens i Einträge mit β gemeinsam hat (allerdings fordern wir nicht, dass die Einträge von $\gamma^{(i)}$ absteigend geordnet sein müssen). Dafür benutzen wir Induktion. Für den Induktionsanfang setzen wir $\gamma^{(0)} := \alpha$ und es ist nichts zu beweisen. Für den Induktionsschritt nehmen wir an, dass $\gamma^{(0)}, \gamma^{(1)}, \dots, \gamma^{(i)}$ bereits konstruiert wurden. Wenn schon $\gamma^{(i)} = \beta$ gilt, setzen wir $\gamma^{(i+1)} := \gamma^{(i)}$ und sind fertig. Ansonsten gibt es einen minimalen Index r mit $\gamma_r^{(i)} > \beta_r$ und einen minimalen Index s mit $\gamma_s^{(i)} < \beta_s$; wegen $\gamma^{(i)} \succcurlyeq \beta$ muss $r > s$ sein. Insbesondere gilt

$$\gamma_r^{(i)} > \beta_r \geq \beta_s > \gamma_s^{(i)}$$

(obwohl $\gamma^{(i)}$ nicht absteigend geordnet sein muss). Sei $\delta := \min\{\gamma_r^{(i)} - \beta_r, \beta_s - \gamma_s^{(i)}\}$. Wir setzen nun $\gamma_r^{(i+1)} := \gamma_r^{(i)} - \delta$ und $\gamma_s^{(i+1)} := \gamma_s^{(i)} + \delta$. Alle anderen Einträge bleiben unverändert. Es ist klar, dass $\gamma^{(i)}$ mindestens einen Eintrag mehr mit β gemeinsam hat als $\gamma^{(i+1)}$, denn es gilt $\gamma_r^{(i)} = \beta_r$ oder $\gamma_s^{(i)} = \beta_s$. Als nächstes zeigen wir $\gamma^{(i)} \succcurlyeq \gamma^{(i+1)} \succcurlyeq \beta$. Die erste Majorisierung ist klar. Für die zweite bemerken wir, dass die gewünschte Ungleichung

$$\gamma_1^{(i+1)} + \gamma_2^{(i+1)} + \dots + \gamma_t^{(i+1)} \geq \beta_1 + \beta_2 + \dots + \beta_t$$

nur für $t \geq s$ verletzt sein kann, denn für kleinere Indizes sind die Einträge von $\gamma^{(i+1)}$ mindestens so groß wie die Einträge von β . Nach Konstruktion gilt aber $\gamma_r^{(i+1)} + \gamma_s^{(i+1)} = \gamma_r^{(i)} + \gamma_s^{(i)}$, sodass für $t \geq s$ die t -te Partialsumme von $\gamma^{(i+1)}$ gleich der t -ten Partialsumme von $\gamma^{(i)}$ ist. Also gilt die gewünschte Ungleichung (bzw. die gewünschte Gleichung für $t = n$) auch in diesem Fall.

Es bleibt zu zeigen, dass auch $\gamma^{(i)} \succcurlyeq' \gamma^{(i+1)}$ gilt. Nach Konstruktion gelten die Ungleichungen

$$\gamma_r^{(i)} > \gamma_r^{(i+1)} \geq \beta_r \geq \beta_s \geq \gamma_s^{(i+1)} > \gamma_s^{(i)}.$$

Insbesondere liegt $\gamma_r^{(i+1)}$ zwischen $\gamma_r^{(i)}$ und $\gamma_s^{(i)}$. Also gibt es eine reelle Zahl $0 < \theta < 1$ mit $\gamma_r^{(i+1)} = \theta \gamma_r^{(i)} + (1 - \theta) \gamma_s^{(i)}$. Weil aber auch $\gamma_r^{(i+1)} + \gamma_s^{(i+1)} = \gamma_r^{(i)} + \gamma_s^{(i)}$ gilt, muss automatisch $\gamma_s^{(i+1)} = (1 - \theta) \gamma_r^{(i)} + \theta \gamma_s^{(i)}$ sein. Indem wir unsere Matrix $\Lambda^{(i)} = (\lambda_{k,j}^{(i)})$ so wählen, dass $\lambda_{r,r}^{(i)} = \lambda_{s,s}^{(i)} = \theta$, $\lambda_{r,s}^{(i)} = \lambda_{s,r}^{(i)} = 1 - \theta$ sowie $\lambda_{k,k}^{(i)} = 1$ für alle $k \neq r, s$ gilt und alle anderen Einträge 0 sind, sehen wir, dass die Bedingung aus (1) erfüllt ist und somit in der Tat $\gamma^{(i)} \succcurlyeq' \gamma^{(i+1)}$ gilt. Das beendet den Induktionsschritt und damit den Beweis von (1).

Beweis von (2). Wir werden eine Folge $\Lambda = \Lambda^{(0)}, \Lambda^{(1)}, \dots, \Lambda^{(n^2)} = 0$ von Matrizen mit nichtnegativen reellen Einträgen konstruieren, sodass mindestens i Einträge von $\Lambda^{(i)}$ gleich 0 sind und $\Lambda^{(i+1)} = \Lambda^{(i)} - \mu_i P_{\sigma_i}$ für eine nichtnegative reelle Zahl $\mu_i \geq 0$ und eine Permutationsmatrix P_{σ_i} gilt. Dann gilt $\Lambda = \sum_{i=1}^{n^2} \mu_i P_{\sigma_i}$. Weil die Summe der Einträge in jeder Zeile und Spalte von

⁶Wenn ihr schon mit Matrizen vertraut seid, bemerkt ihr sicherlich, dass wir hier lediglich die Gleichungen $\gamma = \Lambda' \cdot \alpha$ und $\beta = \Lambda'' \cdot \gamma$ zu der Gleichung $\beta = \Lambda \cdot \alpha$ mit $\Lambda = \Lambda'' \cdot \Lambda'$ umgeformt haben.

$\mu_i P_{\sigma_i}$ gleich μ_i ist, muss außerdem $\sum_{i=1}^n \mu_i = 1$ gelten. Indem wir die Summanden für gleiche σ_i zusammenfassen, erhalten wir also eine Zerlegung $\Lambda = \sum_{\sigma \in \mathfrak{S}_n} \mu_\sigma P_\sigma$ von der gewünschten Form.

Um die Folge von Matrizen zu konstruieren, benutzen wir wieder Induktion. Für den Induktionsanfang setzen wir $\Lambda^{(0)} := \Lambda$ und es ist nichts zu zeigen. Für den Induktionsschritt nehmen wir an, dass $\Lambda^{(0)}, \Lambda^{(1)}, \dots, \Lambda^{(i)}$ bereits konstruiert wurden. Wenn alle Einträge von $\Lambda^{(i)}$ gleich 0 sind, setzen wir $\Lambda^{(i+1)} := \Lambda^{(i)}$ und sind fertig. Ansonsten gibt es mindestens einen positiven Eintrag. Wegen $\Lambda^{(i)} = \Lambda - \sum_{j=1}^i \mu_j P_{\sigma_j}$ ist die Summe der Einträge in jeder Zeile und Spalte von $\Lambda^{(i)}$ gleich $1 - \sum_{j=1}^i \mu_j$. Diese Summe muss positiv sein, sonst wären alle Einträge 0. Aus dem Heiratssatz, oder genauer, aus dem gleichen Argument wie in Aufgabe 2 aus Kapitel 7: *Der Heiratssatz*, folgt, dass wir n positive Einträge auswählen können, sodass in jeder Zeile und jeder Spalte genau einer dieser ausgewählten Einträge liegt. Diese Auswahl wird durch eine Permutation $\sigma_{i+1} \in \mathfrak{S}_n$ beschrieben, sodass wir in der k -ten Zeile den $\sigma_{i+1}(k)$ -ten Eintrag ausgewählt haben. Wenn μ_{i+1} das Minimum der ausgewählten Einträge ist, dann sind alle Einträge von $\Lambda^{(i+1)} := \Lambda^{(i)} - \mu_{i+1} P_{\sigma_{i+1}}$ nichtnegativ, außerdem hat $\Lambda^{(i+1)}$ mindestens einen 0-Eintrag mehr als $\Lambda^{(i)}$. Das beendet den Induktionsschritt und den Beweis von (2). \square

Beweis der Muirhead-Ungleichung. Wähle Gewichte μ_σ wie im Majorisierungs-Lemma. Aus der gewichteten AM-GM-Ungleichung folgt dann

$$\sum_{\sigma \in \mathfrak{S}_n} \mu_\sigma x_1^{\alpha_{\sigma(1)}} x_2^{\alpha_{\sigma(2)}} \dots x_n^{\alpha_{\sigma(n)}} \geq \prod_{\sigma \in \mathfrak{S}_n} x_1^{\mu_\sigma \alpha_{\sigma(1)}} x_2^{\mu_\sigma \alpha_{\sigma(2)}} \dots x_n^{\mu_\sigma \alpha_{\sigma(n)}} = x_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n}.$$

Analoge Ungleichungen gelten auch für alle Vertauschungen der Exponenten $\beta_1, \beta_2, \dots, \beta_n$. Wenn wir alle diese Ungleichungen addieren, steht auf der rechten Seite offensichtlich $T_\beta(x_1, x_2, \dots, x_n)$ und wegen $\sum_{\sigma \in \mathfrak{S}_n} \mu_\sigma = 1$ steht auf der linken Seite genau $T_\alpha(x_1, x_2, \dots, x_n)$.

Gleichheit kann nur eintreten, wenn in jeder gewichteten AM-GM-Ungleichung Gleichheit eingetreten ist, aber diese Bedingung ist sehr unhandlich. Stattdessen erinnern wir uns an die Folge $\alpha = \gamma^{(0)}, \gamma^{(1)}, \dots, \gamma^{(n)} = \beta$ aus dem Beweis des Majorisierungs-Lemmas. Mit Behauptung (2) aus dem Beweis des Majorisierungs-Lemmas können wir analog zu oben zeigen, dass $T_{\gamma^{(i)}}(x_1, x_2, \dots, x_n) \geq T_{\gamma^{(i+1)}}(x_1, x_2, \dots, x_n)$ gelten muss, auch wenn die $\gamma^{(i)}$ nicht absteigend geordnet sein müssen. Insbesondere kann $T_\alpha(x_1, x_2, \dots, x_n) = T_\beta(x_1, x_2, \dots, x_n)$ nur gelten, wenn in jeder der Ungleichungen $T_{\gamma^{(i)}}(x_1, x_2, \dots, x_n) \geq T_{\gamma^{(i+1)}}(x_1, x_2, \dots, x_n)$ Gleichheit eintritt. Diese Ungleichung lässt sich als Summe von Ungleichungen der Form

$$\left(x_{\tau(r)}^{\gamma_r^{(i)}} x_{\tau(s)}^{\gamma_s^{(i)}} + x_{\tau(r)}^{\gamma_s^{(i)}} x_{\tau(s)}^{\gamma_r^{(i)}} \right) \prod_{\substack{k=1 \\ k \neq r, s}}^n x_{\tau(k)}^{\gamma_k^{(i)}} \geq \left(x_{\tau(r)}^{\gamma_r^{(i)} - \delta} x_{\tau(s)}^{\gamma_s^{(i)} + \delta} + x_{\tau(r)}^{\gamma_s^{(i)} + \delta} x_{\tau(s)}^{\gamma_r^{(i)} - \delta} \right) \prod_{\substack{k=1 \\ k \neq r, s}}^n x_{\tau(k)}^{\gamma_k^{(i)}}$$

für Permutationen $\tau \in \mathfrak{S}_n$ schreiben. Wenn alle Variablen positiv sind, können wir die Produkte ignorieren und Gleichheit kann nur eintreten, wenn die Ausdrücke in den Klammern gleich sind. Für $\alpha \neq \beta$ kommt es mindestens einmal vor, dass $\delta > 0$ ist. Dann kann Gleichheit nur für $x_{\tau(r)} = x_{\tau(s)}$ gelten. Weil τ eine beliebige Permutation war, folgt $x_1 = x_2 = \dots = x_n$, wie gewünscht. \square

Die Schur-Ungleichung

Manchmal lassen sich Ungleichungen nicht mit Muirhead beweisen, obwohl sie sehr danach aussehen. So zum Beispiel die Ungleichung

$$x^3 + y^3 + z^3 + 3xyz \geq x^2y + xy^2 + y^2z + yz^2 + z^2x + zx^2$$

für alle $x, y, z \geq 0$ (diese Ungleichung ist tatsächlich wahr, wie wir sogleich sehen werden). Wenn wir sie in der Notation $\frac{1}{2}T_{(3,0,0)}(x, y, z) + \frac{1}{2}T_{(1,1,1)}(x, y, z) \geq T_{(2,1,0)}(x, y, z)$ schreiben, sehen wir, dass zwar $(3, 0, 0) \succ (2, 1, 0)$ gilt, aber auch $(1, 1, 1) \prec (2, 1, 0)$. Also ist Muirhead nicht anwendbar. Auch gewichtetes AM-GM wird hier versagen. Denn egal, was für Gewichte wir wählen, solange xyz mit positivem Gewicht vorkommt, können wir nur gegen Terme abschätzen, die alle drei Variablen enthalten. Also müssten wir $x^3 + y^3 + z^3$ allein gegen den Term auf der rechten Seite abschätzen, was offensichtlich nicht klappen kann.

Glücklicherweise schafft die Schur-Ungleichung in solchen Situationen Abhilfe!

Schur-Ungleichung. Sei $I \subseteq \mathbb{R}$ ein Intervall und $f: I \rightarrow \mathbb{R}_{\geq 0}$ eine Funktion mit nichtnegativen reellen Werten. Angenommen, f ist monoton (sowohl steigend als auch fallend ist erlaubt) oder konvex (siehe Kapitel 3: Die Ungleichungen von Jensen und Karamata). Dann gilt für alle $x, y, z \in I$

$$f(x)(x-y)(x-z) + f(y)(y-z)(y-x) + f(z)(z-x)(z-y) \geq 0.$$

Beweis. Weil die Ungleichung symmetrisch in x, y und z ist, dürfen wir ohne Einschränkung $x \geq y \geq z$ annehmen. Wenn f monoton steigend ist, können wir die Ungleichung wie folgt umschreiben:

$$(x-y)(f(x)(x-z) - f(y)(y-z)) + f(z)(x-z)(y-z) \geq 0.$$

Nach Annahme ist $f(x) \geq f(y)$ und $x-z \geq y-z$, also ist der erste Summand nichtnegativ. Der zweite Summand ist ebenfalls nichtnegativ. Also gilt die gewünschte Ungleichung. Wenn f monoton fallend ist, können wir analog mit z statt x argumentieren.

Es bleibt der Fall, dass f konvex ist. In diesem Fall verwenden wir die gewichtete Jensen-Ungleichung (siehe Kapitel 3: Die Ungleichungen von Jensen und Karamata) und erhalten

$$f(y) = f\left(\frac{y-z}{x-z}x + \frac{x-y}{x-z}z\right) \leq \frac{y-z}{x-z}f(x) + \frac{x-y}{x-z}f(z)$$

(wegen $x \geq y \geq z$ liegen die Gewichte auch tatsächlich im Intervall $[0, 1]$). Einsetzen liefert

$$\begin{aligned} & f(x)(x-y)(x-z) - f(y)(y-z)(x-y) + f(z)(x-z)(y-z) \\ & \geq (x-y)f(x)\frac{(x-z)^2 - (y-z)^2}{x-z} + (y-z)f(z)\frac{(x-z)^2 - (x-y)^2}{x-z} \geq 0, \end{aligned}$$

denn wiederum sind beide Summanden aufgrund unserer Annahme $x \geq y \geq z$ positiv. \square

Meistens wird die Schur-Ungleichung auf Funktionen der Form $f(x) = x^\alpha$ für eine reelle Zahl α angewendet. Häufig wird sogar nur der Fall $\alpha = 1$ betrachtet. In diesem Fall erhalten wir die anfangs behauptete Ungleichung $x^3 + y^3 + z^3 + 3xyz \geq x^2y + xy^2 + y^2z + yz^2 + z^2x + zx^2$. Diesen Spezialfall solltet ihr euch auf jeden Fall merken!

Beispielaufgaben

Ihr sollt nun die Schurhead-Methode selbstständig auf zwei Aufgaben anwenden. Wie üblich findet ihr unter den Beispielaufgaben Tipps und am Ende des Heftes Musterlösungen.

Aufgabe 1. Gegeben seien nichtnegative reelle Zahlen $x, y, z \geq 0$ mit $x + y + z = 1$. Beweise die Ungleichung

$$0 \leq xy + yz + zx - 2xyz \leq \frac{7}{27}.$$

(Aufgabe 1 haben wir schon im Heft für Klasse 9 mit der Schiebemethode gelöst. Hier sollt ihr euch einen weiteren Beweis mit der Schurhead-Ungleichung überlegen.)

Aufgabe 2. Beweise, dass für nichtnegative reelle Zahlen $x, y, z \geq 0$ stets die folgende Ungleichung gilt:

$$(xy + yz + zx)(x^2 + y^2 + z^2) + 3(x^4 + y^4 + z^4) \geq 6(x^2y^2 + y^2z^2 + z^2x^2)$$

Tipps zu den Beispielaufgaben

Tipp zu Aufgabe 1. Homogenisiere die Ungleichung.

Tipp zu Aufgabe 2. Multipliziere die Schur-Ungleichung mit $x + y + z$.

3 Die Ungleichungen von Jensen und Karamata

Es kommt recht häufig vor, dass in einer Ungleichung die Variablen „getrennt“ vorliegen, sodass wir die Ungleichung in der Form $f(x_1) + f(x_2) + \dots + f(x_n) \geq c$ schreiben können. Hierbei ist f eine geeignete Funktion, x_1, x_2, \dots, x_n sind Variablen (möglicherweise mit einer Nebenbedingung) und c ist eine Konstante.

Die Jensensche Ungleichung liefert eine Lösungsmethode unter der Voraussetzung, dass f *konvex* ist. Im Heft für die Klasse 11 werdet ihr einige Tricks kennenlernen, mit der sich die Jensensche Ungleichung sogar auf manche nicht-konvexe Funktionen anwenden lässt.

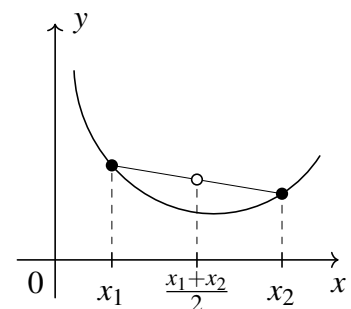
Konvexe Funktionen und die Jensensche Ungleichung

Definition. Sei $I \subseteq \mathbb{R}$ ein Intervall. Eine stetige Funktion $f: I \rightarrow \mathbb{R}$ heißt *konvex*, wenn für alle $x_1, x_2 \in I$ die folgende Ungleichung gilt:

$$\frac{f(x_1) + f(x_2)}{2} \geq f\left(\frac{x_1 + x_2}{2}\right).$$

Umgekehrt heißt f *konkav*, wenn die obige Ungleichung mit „ \leq “ statt „ \geq “ gilt.

Anschaulich bedeutet konvex zu sein, dass für jede Strecke zwischen zwei Punkten auf dem Funktionsgraphen von f der Mittelpunkt dieser Strecke stets oberhalb des Graphen oder auf dem Graphen liegt, aber niemals unterhalb. Indem wir uns die Graphen dieser Funktionen anschauen, sieht es zum Beispiel so aus, als wäre $f(x) = x^{2n}$ für jede positive ganze Zahl $n \geq 1$ auf ganz \mathbb{R} konvex. Hingegen sollte $g(x) = x^{2n-1}$ für $x \geq 0$ konvex und für $x \leq 0$ konkav sein. Und als letztes Beispiel sieht $h(x) = \sin(x)$ im Intervall $[0, 180^\circ]$ konkav aus.



konvexe Funktion

Alle diese Funktionen sind auch tatsächlich konvex/konkav wie angegeben. Dies mit der Definition zu beweisen, wäre allerdings reichlich mühsam. Glücklicherweise gibt es ein einfacheres Kriterium.

Lemma. Sei $f: I \rightarrow \mathbb{R}$ eine Funktion, die im Inneren von I zweifach differenzierbar ist (am Rand von I muss die Ableitung von f nicht existieren). Die Funktion f ist genau dann konvex, wenn ihre zweite Ableitung f'' überall nichtnegativ ist: $f''(x) \geq 0$ für alle inneren Punkte $x \in I$. Umgekehrt ist f genau dann konkav, wenn f'' überall nichtpositiv ist.

Wir werden dieses Kriterium nicht beweisen (nicht zuletzt, weil die Differentialrechnung erst Stoff der Klasse 11 ist), aber hier ist zumindest ein Plausibilitätsargument: Intuitiv bedeutet konvex zu sein, dass die Tangenten an den Funktionsgraphen von f immer steiler oder zumindest nicht flacher werden. Das bedeutet, dass die erste Ableitung f' monoton steigend ist. Das wiederum bedeutet, dass die zweite Ableitung f'' nichtnegativ ist.

Nun werden wir die Ungleichung, die diesem Kapitel seinen Namen gibt, beweisen.

Jensensche Ungleichung. Gegeben seien eine konvexe Funktion $f: I \rightarrow \mathbb{R}$ und reelle Zahlen $x_1, x_2, \dots, x_n \in I$. Dann gilt die Ungleichung

$$\frac{f(x_1) + f(x_2) + \dots + f(x_n)}{n} \geq f\left(\frac{x_1 + x_2 + \dots + x_n}{n}\right).$$

Wenn f stattdessen konkav ist, gilt eine analoge Ungleichung mit „ \leq “ statt „ \geq “.

Analog zur Definition von Konvexität lässt sich die Jensensche Ungleichung geometrisch veranschaulichen: Für jedes n -Eck, dessen Eckpunkte auf dem Funktionsgraphen von f liegen, liegt der Schwerpunkt dieses n -Ecks oberhalb des Graphen oder auf dem Graphen. Tatsächlich befindet sich sogar das komplette n -Eck oberhalb des Graphen oder auf dem Graphen von f . Das führt uns sofort auf eine gewichtete Verallgemeinerung der Jensenschen Ungleichung:

Gewichtete Jensen-Ungleichung. Gegeben seien eine konvexe Funktion $f: I \rightarrow \mathbb{R}$, reelle Zahlen $x_1, x_2, \dots, x_n \in I$ sowie Gewichte $\lambda_1, \lambda_2, \dots, \lambda_n \geq 0$ mit $\lambda_1 + \lambda_2 + \dots + \lambda_n = 1$. Dann gilt

$$\lambda_1 f(x_1) + \lambda_2 f(x_2) + \dots + \lambda_n f(x_n) \geq f(\lambda_1 x_1 + \lambda_2 x_2 + \dots + \lambda_n x_n).$$

Wenn f stattdessen konkav ist, gilt eine analoge Ungleichung mit „ \leq “ statt „ \geq “.

Beweis. Mit einer einfachen Induktion über k zeigen wir zuerst, dass für alle $x_1, x_2, \dots, x_{2^k} \in I$ die Ungleichung

$$\frac{f(x_1) + f(x_2) + \dots + f(x_{2^k})}{2^k} \geq f\left(\frac{x_1 + x_2 + \dots + x_{2^k}}{2^k}\right)$$

gilt (also dass die ungewichtete Jensen-Ungleichung für $n = 2^k$ erfüllt ist).

Als nächstes zeigen wir die gewichtete Jensen-Ungleichung in dem Spezialfall, dass alle λ_i rationale Zahlen sind, deren Nenner allesamt Zweierpotenzen sind. Indem wir alle λ_i auf einen Hauptnenner bringen, können wir $\lambda_i = m_i/2^k$ für gewisse nichtnegative ganze Zahlen m_i schreiben. Die Bedingung $\lambda_1 + \lambda_2 + \dots + \lambda_n = 1$ impliziert $m_1 + m_2 + \dots + m_n = 2^k$. Indem wir die Jensensche Ungleichung (in dem Spezialfall, in dem wir sie schon bewiesen haben) auf m_1 mal x_1 , m_2 mal x_2 , ..., m_n mal x_n anwenden, erhalten wir die behauptete Ungleichung $\lambda_1 f(x_1) + \lambda_2 f(x_2) + \dots + \lambda_n f(x_n) \geq f(\lambda_1 x_1 + \lambda_2 x_2 + \dots + \lambda_n x_n)$.

Der allgemeine Fall folgt aus einem Stetigkeitsargument. Angenommen, die Ungleichung wäre falsch. Dann gilt also $\lambda_1 f(x_1) + \lambda_2 f(x_2) + \dots + \lambda_n f(x_n) = f(\lambda_1 x_1 + \lambda_2 x_2 + \dots + \lambda_n x_n) - \varepsilon$ für ein $\varepsilon > 0$. Wir können $\lambda_1, \lambda_2, \dots, \lambda_n$ beliebig genau durch rationale Zahlen $\lambda'_1, \lambda'_2, \dots, \lambda'_n$ approximieren, deren Nenner Zweierpotenzen sind. Weil f stetig ist (das war Teil unserer Definition von Konvexität), wird dann auch der Funktionswert $f(\lambda_1 x_1 + \lambda_2 x_2 + \dots + \lambda_n x_n)$ beliebig genau durch $f(\lambda'_1 x_1 + \lambda'_2 x_2 + \dots + \lambda'_n x_n)$ approximiert. Indem wir genau genug approximieren, können wir rationale Gewichte $\lambda'_1, \lambda'_2, \dots, \lambda'_n$ mit Zweierpotenzen als Nenner und $\lambda'_1 + \lambda'_2 + \dots + \lambda'_n = 1$ finden, sodass Folgendes gilt:

$$\begin{aligned} |(\lambda_1 f(x_1) + \lambda_2 f(x_2) + \dots + \lambda_n f(x_n)) - (\lambda'_1 f(x_1) + \lambda'_2 f(x_2) + \dots + \lambda'_n f(x_n))| &< \frac{\varepsilon}{2} \\ |f(\lambda_1 x_1 + \lambda_2 x_2 + \dots + \lambda_n x_n) - f(\lambda'_1 x_1 + \lambda'_2 x_2 + \dots + \lambda'_n x_n)| &< \frac{\varepsilon}{2}. \end{aligned}$$

Da wir die Jensensche Ungleichung für die Gewichte $\lambda'_1, \lambda'_2, \dots, \lambda'_n$ bereits bewiesen haben, folgt nun aber

$$\lambda_1 f(x_1) + \lambda_2 f(x_2) + \dots + \lambda_n f(x_n) - f(\lambda_1 x_1 + \lambda_2 x_2 + \dots + \lambda_n x_n) > -\frac{\varepsilon}{2} - \frac{\varepsilon}{2} = -\varepsilon.$$

Das widerspricht unserer Wahl von ε . Unsere Annahme, dass die gewichtete AM-GM-Ungleichung falsch wäre, muss also selber falsch gewesen sein. \square

Die Ungleichung von Karamata

Die Ungleichung von Karamata ist eine weitere Verallgemeinerung der Jensenschen Ungleichung. Hierfür benötigen wir das Konzept der *Majorisierung*, das ihr in Kapitel 2: *Die Schurhead-Ungleichung* kennengelernt haben. Weil ein beliebiges absteigend geordnetes n -Tupel (x_1, \dots, x_n) ,

$x_1 \geq x_2 \geq \dots \geq x_n$, stets das n -Tupel $(\frac{x_1+\dots+x_n}{n}, \frac{x_1+\dots+x_n}{n}, \dots, \frac{x_1+\dots+x_n}{n})$ majorisiert, lässt sich die Jensensche Ungleichung aus der Ungleichung von Karamata zurückerhalten.

Ungleichung von Karamata. Gegeben sei eine konvexe Funktion $f: I \rightarrow \mathbb{R}$ sowie absteigend geordnete n -Tupel $x_1 \geq x_2 \geq \dots \geq x_n$ und $y_1 \geq y_2 \geq \dots \geq y_n$ von Elementen von I . Angenommen, es gilt $(x_1, x_2, \dots, x_n) \succ (y_1, y_2, \dots, y_n)$. Dann gilt die folgende Ungleichung:

$$f(x_1) + f(x_2) + \dots + f(x_n) \geq f(y_1) + f(y_2) + \dots + f(y_n).$$

Wenn f stattdessen konkav ist, gilt eine analoge Ungleichung mit „ \leq “ statt „ \geq “.

Beweis. Nach dem Majorisierungs-Lemma (siehe Kapitel 2: Die Schurhead-Ungleichung) gibt es Gewichte $\mu_\sigma \geq 0$, $\sigma \in \mathfrak{S}_n$, mit $\sum_{\sigma \in \mathfrak{S}_n} \mu_\sigma = 1$ und $y_i = \sum_{\sigma \in \mathfrak{S}_n} \mu_\sigma x_{\sigma(i)}$. Indem wir die gewichtete Jensen-Ungleichung mit den Gewichten μ_σ anwenden, erhalten wir

$$\sum_{\sigma \in \mathfrak{S}_n} \mu_\sigma f(x_{\sigma(i)}) \geq f\left(\sum_{\sigma \in \mathfrak{S}_n} \mu_\sigma x_{\sigma(i)}\right) = f(y_i)$$

für alle $i = 1, 2, \dots, n$. Wenn wir alle diese Ungleichungen addieren, steht auf der rechten Seite offensichtlich $f(y_1) + f(y_2) + \dots + f(y_n)$ und wegen $\sum_{\sigma \in \mathfrak{S}_n} \mu_\sigma = 1$ steht auf der linken Seite genau $f(x_1) + f(x_2) + \dots + f(x_n)$. Das beendet den Beweis. \square

Beispielaufgaben

Wie üblich findet ihr weiter unten Tipps und am Ende des Heftes Musterlösungen zu den Übungsaufgaben. Aufgabe 2 ist ziemlich schwierig, aber sie lehrt euch einen coolen Trick, den ihr euch merken solltet.

Aufgabe 1. Gegeben seien positive reelle Zahlen $a_1, a_2, \dots, a_n \geq 0$.

(a) Benutze die Jensensche Ungleichung, um die AM-GM-Ungleichung zu zeigen:

$$\frac{a_1 + a_2 + \dots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \dots a_n}.$$

(b) Benutze die Jensensche Ungleichung, um die allgemeine Potenzmittelungleichung zu zeigen: Für positive reelle Zahlen $p > q > 0$ gilt stets

$$\left(\frac{a_1^p + a_2^p + \dots + a_n^p}{n}\right)^{1/p} \geq \left(\frac{a_1^q + a_2^q + \dots + a_n^q}{n}\right)^{1/q}.$$

Aufgabe 2.** Gegeben seien $a, b, c > 0$ positive reelle Zahlen mit $a^2 + b^2 + c^2 \geq 3$. Zeige, dass

$$\frac{(a+1)(b+2)}{(b+1)(b+5)} + \frac{(b+1)(c+2)}{(c+1)(c+5)} + \frac{(c+1)(a+2)}{(a+1)(a+5)} \geq \frac{3}{2}$$

Tipps zu den Beispielaufgaben

Tipps zu Aufgabe 1. Benutze die Jensensche Ungleichung für die Funktionen $f(x) = e^x$ und $g(x) = x^{p/q}$. Kannst du zeigen, dass diese Funktionen konkav oder konvex sind?

Tipps zu Aufgabe 2. Interpretiere die Terme auf der linken Seite teilweise als Gewichte und teilweise als Funktion. Dann benutze die gewichtete Jensen-Ungleichung.

4 Potenzgeraden

In diesem Kapitel lernt ihr eine Konstruktion und mehrere nützliche Sätze kennen, die häufig in den Lösungen von schweren Geometrie-Aufgaben vorkommen.

Definition. Sei Ω ein Kreis mit Mittelpunkt O und Radius r . Sei X ein Punkt. Die *Potenz von X bezüglich Ω* ist $\text{Pot}_\Omega(X) := |OX|^2 - r^2$.

Eigenschaften der Potenz. Die Potenz von X bezüglich Ω lässt sich alternativ auch folgendermaßen beschreiben:

- (a) Wenn eine Gerade durch X den Kreis Ω in zwei Punkten A und B schneidet, dann gilt (mit gerichteten Streckenlängen) $\text{Pot}_\Omega(X) = AX \cdot BX$.
- (b) Wenn X außerhalb von Ω liegt und T der Berührungspunkt einer Tangente durch X an Ω ist, dann gilt $\text{Pot}_\Omega(X) = |TX|^2$.

Beweis. Nach dem Sehensatz bzw. dem Sekantensatz ist das Produkt $AX \cdot BX$ unabhängig von der Wahl der Geraden durch X . Es genügt also, die Gleichung $\text{Pot}_\Omega(X) = AX \cdot BX$ für eine einzige Wahl der Geraden durch X zu zeigen. Dazu wählen wir die Gerade durch O und X , sodass A und B die beiden Schnittpunkte von OX mit Ω sind. Dann gilt

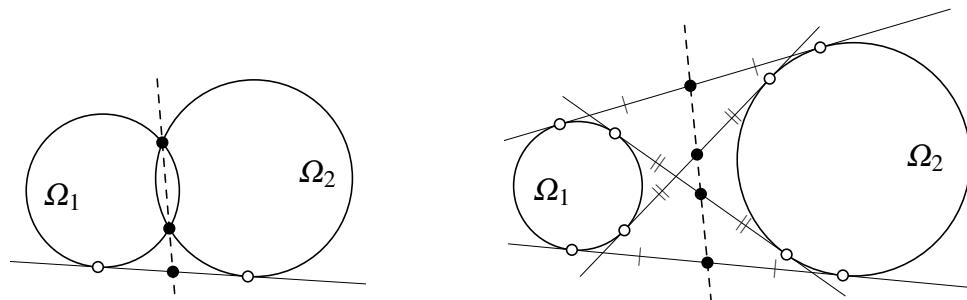
$$AX \cdot BX = (OX + r)(OX - r) = |OX|^2 - r^2$$

nach der dritten binomischen Formel. Das zeigt Eigenschaft (a). Eigenschaft (b) folgt sofort aus Eigenschaft (a) und dem Sekanten-Tangentensatz. \square

Potenzgerade zweier Kreise. Seien Ω_1 und Ω_2 zwei nicht-konzentrische Kreise mit den (verschiedenen) Mittelpunkten O_1 und O_2 sowie den Radien r_1 und r_2 . Dann ist die Menge aller Punkte X , für die $\text{Pot}_{\Omega_1}(X) = \text{Pot}_{\Omega_2}(X)$ gilt, eine Gerade, die senkrecht auf O_1O_2 steht.

Beweis. Sei X ein Punkt in der Ebene und sei X' der Lotfußpunkt von X auf O_1O_2 . Nach dem Satz des Pythagoras gilt dann $|O_1X|^2 = |O_1X'|^2 + |XX'|^2$ und $|O_2X|^2 = |O_2X'|^2 + |XX'|^2$. Also gilt $\text{Pot}_{\Omega_1}(X) = \text{Pot}_{\Omega_2}(X)$ genau dann, wenn $\text{Pot}_{\Omega_1}(X') = \text{Pot}_{\Omega_2}(X')$ gilt. Es genügt also, zu zeigen, dass auf der Gerade O_1O_2 genau ein Punkt X' existiert, für den $\text{Pot}_{\Omega_1}(X') = \text{Pot}_{\Omega_2}(X')$ gilt (und die gesuchte Menge ist dann automatisch die Senkrechte auf O_1O_2 in X').

Seien $x := O_1X'$ und $d := O_1O_2$, wobei wir gerichtete Streckenlängen verwenden. Dann gilt $O_2X' = O_1X' - O_1O_2 = x - d$. Die Gleichung $\text{Pot}_{\Omega_1}(X') = \text{Pot}_{\Omega_2}(X')$ ist somit äquivalent zu $x^2 - r_1^2 = (x - d)^2 - r_2^2$. Hierin kürzen sich die quadratischen Terme und wir erhalten als einzige Lösung $x = (r_2^2 - r_1^2 - d^2)/(2d)$ (beachte, dass $d \neq 0$ gilt, da wir angenommen haben, dass Ω_1 und Ω_2 nicht konzentrisch sind). Damit ist gezeigt, dass auf der Gerade O_1O_2 in der Tat genau ein X' mit $\text{Pot}_{\Omega_1}(X') = \text{Pot}_{\Omega_2}(X')$ existiert und wir sind fertig. \square



Die Potenzgerade von Ω_1 und Ω_2 in zwei Fällen.

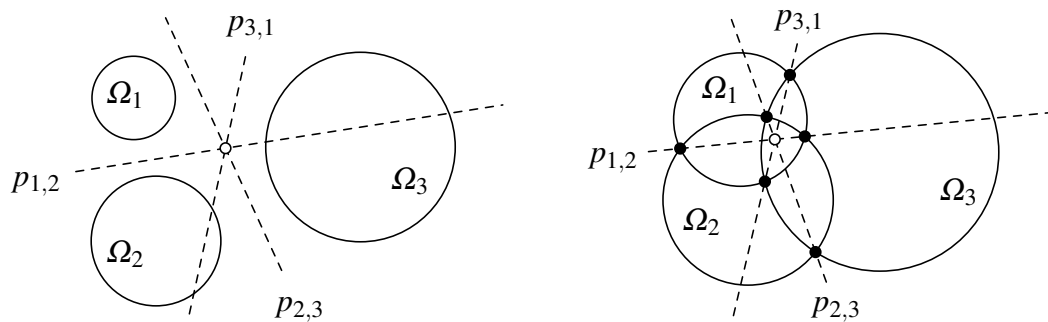
Potenzgeraden sind interessant, weil einige kanonisch auftretende Punkte auf ihnen liegen. Wenn sich Ω_1 und Ω_2 zum Beispiel in zwei Punkten P und Q schneiden, dann liegen P und Q beide

auf der Potenzgeraden von Ω_1 und Ω_2 , denn sie haben Potenz 0 bezüglich beider Kreise. In diesem Fall ist die Potenzgerade also einfach die Gerade PQ . Sei ferner t eine gemeinsame Tangente an Ω_1 und Ω_2 mit Berührungspunkten T_1, T_2 . Wenn sich Ω_1 und Ω_2 schneiden, kommen für t nur die beiden äußeren gemeinsamen Tangenten in Frage. Wenn sich Ω_1 und Ω_2 hingegen nicht schneiden, können wir für t auch die beiden inneren gemeinsamen Tangenten wählen. In jedem Fall liegt der Mittelpunkt von $\overline{T_1 T_2}$ auf der Potenzgeraden, was sofort aus der zweiten alternativen Beschreibung folgt.

Außerdem haben wir den folgenden, sehr nützlichen Fakt:

Potenzzentrum dreier Kreise. Seien Ω_1, Ω_2 und Ω_3 drei paarweise nicht-konzentrische Kreise. Sei $p_{1,2}$ die Potenzgerade von Ω_1 und Ω_2 und definiere $p_{2,3}, p_{3,1}$ analog. Dann schneiden sich $p_{1,2}, p_{2,3}$ und $p_{3,1}$ in einem Punkt (oder sind paarweise parallel).

Insbesondere gilt: Wenn sich die Kreise Ω_1, Ω_2 und Ω_3 paarweise schneiden, dann treffen sich die drei Verbindungsgeraden der Schnittpunkte in einem Punkt (oder sind paarweise parallel).

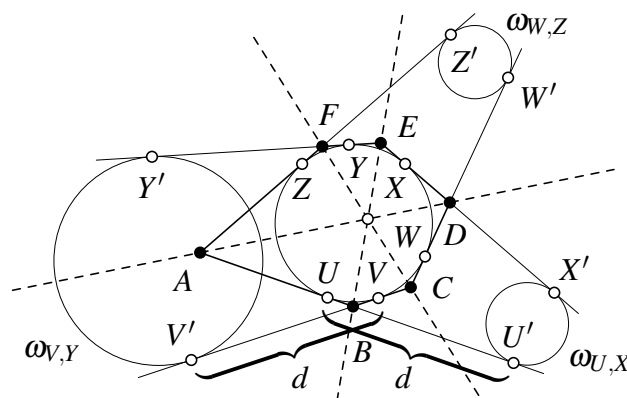


Die paarweisen Potenzgeraden von Ω_1, Ω_2 und Ω_3 in zwei Fällen.

Beweis. Wenn die drei Potenzgeraden nicht paarweise parallel sind, dürfen wir ohne Beschränkung der Allgemeinheit annehmen, dass sich $p_{1,2}$ und $p_{2,3}$ in einem Punkt Z schneiden. Dann hat Z die gleiche Potenz bezüglich Ω_1, Ω_2 und Ω_3 . Also liegt Z auch auf $p_{2,3}$. \square

Wir wollen nun Potenzgeraden benutzen, um einen Satz über Tangentensechsecke zu beweisen.

Satz von Brianchon. Sei $ABCDEF$ ein konvexes Tangentensechseck. Dann schneiden sich die Hauptdiagonalen AD, BE und CF in einem Punkt.

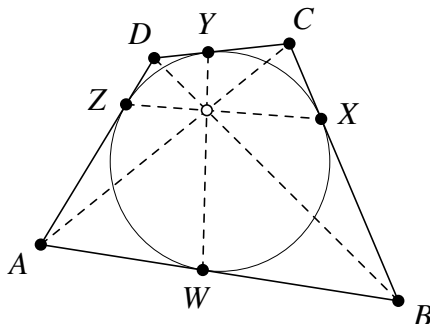


Beweis. Wir wollen AD, BE und CF als Potenzgeraden von geeigneten Kreisen interpretieren. Dazu sei ω der Inkreis; die Berührungspunkte mit den Seiten des Tangentensechsecks bezeichnen wir in dieser Reihenfolge mit U, V, W, X, Y, Z , sodass U auf \overline{AB} liegt, V auf \overline{BC} und so weiter. Wähle außerdem eine hinreichend große Länge $d > 0$. Dann gibt es auf der Verlängerung von \overline{AB} über B hinaus einen Punkt U' mit $|UU'| = d$ und auf der Verlängerung von \overline{BC} über B hinaus einen Punkt V' mit $|VV'| = d$. Analog wählen wir Punkte W' und X' auf den Verlängerungen

von \overline{CD} und \overline{DE} über D hinaus sowie Y' und Z' auf den Verlängerungen von \overline{EF} und \overline{FA} über F hinaus. Dann gibt es einen Kreis $\omega_{U,X}$, der die Gerade AB in U' und die Gerade DE in X' berührt. Analog definieren wir Kreise $\omega_{V,Y}$ und $\omega_{W,Z}$. Die Tangentenabschnitte \overline{BU} und \overline{BV} sind gleich lang. Wegen $|BU'| = d - |BU|$ und $|BV'| = d - |BV|$ folgt, dass auch die Tangentenabschnitte $\overline{BU'}$ und $\overline{BV'}$ gleich lang sind. Nach Eigenschaft (b) liegt B auf der Potenzgeraden der Kreise $\omega_{U,X}$ und $\omega_{V,Y}$. Analoge Überlegungen lassen sich für die anderen Eckpunkte anstellen. Wir erhalten also in der Tat, dass AD , BE und CF die paarweisen Potenzgeraden der Kreise $\omega_{U,X}$, $\omega_{V,Y}$ und $\omega_{W,Z}$ sind. Somit schneiden sie sich in der Tat in einem Punkt (der parallele Fall kann nicht auftreten, da $ABCDEF$ konvex ist). \square

Der Satz von Brianchon ist nicht zuletzt dann nützlich, wenn er auf entartete Tangentensechsecke angewendet wird, in denen ein oder mehrere Eckpunkte auf dem Inkreis liegen (sodass die Innenwinkel an diesen Eckpunkten die Größe 180° haben). Wir erhalten zum Beispiel folgenden bekannten Satz:

Satz. Sei $ABCD$ ein Tangentenviereck und seien W , X , Y und Z die Berührungspunkte des Inkreises mit den Seiten \overline{AB} , \overline{BC} , \overline{CD} und \overline{DA} . Dann schneiden sich die Diagonalen AC und BD sowie die Geraden WY und XZ in einem Punkt.



Beweis. Wende den Satz von Brianchon auf die entarteten Tangentensechsecke $AWBCYD$ und $ABXCDZ$ an. \square

Beispielaufgaben

Wie üblich findet ihr am Ende des Kapitels Tipps und am Ende des Heftes Lösungen zu den Beispielaufgaben.

Aufgabe 1. Gegeben seien Kreise ω_1 und ω_2 , die sich in den Punkten X und Y schneiden. Eine Gerade ℓ_1 durch den Mittelpunkt von ω_1 schneide ω_2 in den Punkten P und Q . Eine Gerade ℓ_2 durch den Mittelpunkt von ω_2 schneide ω_1 in den Punkten R und S . Zeige: Wenn $PQRS$ ein Sehnenviereck ist, dann liegt sein Umkreismittelpunkt auf der Gerade XY .

Aufgabe 2. Die Punkte A , B , C und D liegen in dieser Reihenfolge auf einer Geraden ℓ . Der Kreis ω_1 mit Durchmesser \overline{AC} und der Kreis ω_2 mit Durchmesser \overline{BD} schneiden sich in den Punkten X und Y . Sei Z der Schnittpunkt von XY mit der Strecke \overline{BC} und sei P ein innerer Punkt der Strecke \overline{XZ} . Die Gerade CP schneide ω_1 außer in C noch in einem weiteren Punkt M und die Gerade BP schneide ω_2 außer in B noch in einem weiteren Punkt N . Zeige, dass sich die Geraden AM , DN und XY in einem Punkt schneiden.

Aufgabe 3. Das Dreieck ABC sei bei C gleichschenkelig. Sei M ein innerer Punkt der Strecke \overline{BC} . Auf der Verlängerung von \overline{AM} über M hinaus gebe es einen Punkt N , für den $|AN| = |AC|$ gilt. Die Umkreise $\odot ABC$ und $\odot CMN$ schneiden sich außer in C noch in einem weiteren Punkt P . Sei Q der Schnittpunkt von AB und CP . Zeige, dass Q auch auf der Winkelhalbierenden von $\sphericalangle BMN$ liegt.

Aufgabe 4. Sei $ABCD$ ein Tangentenviereck ist und seien W, X, Y und Z die Berührungspunkte des Inkreises mit den Seiten $\overline{AB}, \overline{BC}, \overline{CD}$ und \overline{DA} . Sei ferner P der Schnittpunkt der Diagonalen AC und BD . Beweise

$$\frac{|AP|}{|CP|} = \frac{|AW|}{|CX|} = \frac{|AZ|}{|CY|}.$$

Tipps zu den Beispielaufgaben

Tipps zu Aufgabe 1. Betrachte die paarweisen Potenzgeraden der Kreise ω_1, ω_2 und $\odot PQRS$.

Wenn O_1, O_2 und O die Mittelpunkte von ω_1, ω_2 und $\odot PQRS$ bezeichnen, dann betrachte den Höhenschnittpunkt des Dreiecks OO_1O_2 .

Tipp zu Aufgabe 2. Zeige, dass $BCNM$ und $ADNM$ Sehnenvierecke sind und benutze den Satz über das Potenzzentrum dreier Kreise.

Tipps zu Aufgabe 3. Zeige, dass AB, CP und die Winkelhalbierende von $\sphericalangle BMN$ die paarweisen Potenzgeraden von $\odot ABC, \odot CMN$ und einem weiteren Kreis sind.

Welcher Kreis könnte dieser weitere Kreis sein? Mach dir eine genaue Skizze und stelle eine Vermutung auf. Beweise diese Vermutung dann mit einer Winkeljagd.

Tipps zu Aufgabe 4. Benutze den Satz von Ceva, um die Behauptung umzuformulieren.

Um die umformulierte Behauptung zu beweisen, kann zum Beispiel der Satz von Brianchon verwendet werden.

5 (Dreh-)Streckungen

Seid ihr gut darin, in einer Skizze ähnliche Dreiecke zu erraten? Der Autor dieses Kapitels definitiv nicht! Wenn euch das genauso geht, dann ist dieses Kapitel genau richtig für euch. Drehstreckungen sind ein sehr nützliches Hilfsmittel, um über geometrische Konfigurationen nachzudenken. Wenn ihr diese Denkweise einmal verinnerlicht habt, wird es euch leichter fallen, ähnliche Dreiecke, kollineare Punkte und andere Beziehungen zu erkennen.

Allgemeine Theorie

Definition. Eine *orientierungserhaltende Ähnlichkeitsabbildung* ist eine Abbildung der Euklidischen Ebene auf sich selber, sodass für beliebige drei Punkte A, B, C und ihre Bildpunkte A', B', C' die Dreiecke ABC und $A'B'C'$ gleichsinnig ähnlich sind.

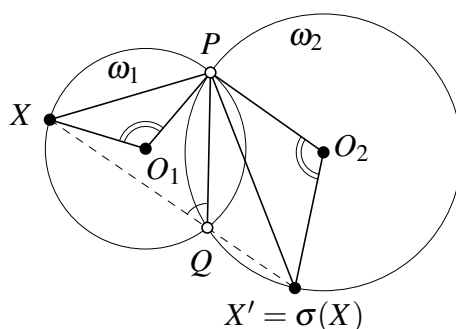
Orientierungserhaltende Ähnlichkeitsabbildungen können folgendermaßen klassifiziert werden:

Klassifikation von orientierungserhaltenden Ähnlichkeitsabbildungen. Jede orientierungserhaltende Ähnlichkeitsabbildung ist eine Drehstreckung oder eine Verschiebung. Ferner gilt:

- (a) Die Hintereinanderausführung von zwei Drehstreckungen (die nicht notwendigerweise das gleiche Zentrum haben müssen) ist wieder eine Drehstreckung oder eine Verschiebung.
- (b) Die Hintereinanderausführung von zwei Streckungen (die nicht notwendigerweise das gleiche Zentrum haben müssen) ist wieder eine Streckung oder eine Verschiebung.
- (c) Die Hintereinanderausführung von zwei Drehungen (die nicht notwendigerweise das gleiche Zentrum haben müssen) ist wieder eine Drehung oder eine Verschiebung.

Zum Beweis benutzen wir ein Lemma, das auch für sich genommen nützlich sein kann.

Lemma. Seien ω_1 und ω_2 zwei Kreise, die sich in P und Q schneiden. Sei σ die Drehstreckung mit Zentrum P , die ω_1 auf ω_2 abbildet. Dann ist σ identisch mit der Projektion durch Q . Das bedeutet: Für jeden Punkt X auf ω_1 ist $\sigma(X)$ der zweite Schnittpunkt von XQ mit ω_2 (im Fall $X = Q$ interpretieren wir XQ als die Tangente an ω_1 in Q).



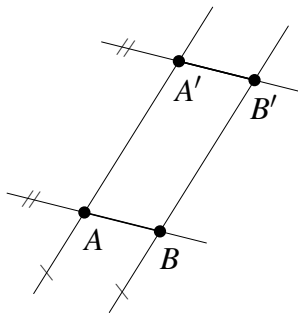
Beweis. Wir betrachten nur den Fall, dass X auf dem Kreisbogen \widehat{PQ} von ω_1 liegt, der außerhalb von ω_2 verläuft; der andere Fall geht analog. Sei X' der zweite Schnittpunkt von XQ mit ω_2 und seien O_1, O_2 die Mittelpunkte von ω_1, ω_2 . Die Drehstreckung σ bildet O_1 auf O_2 ab und P auf sich selbst. Es genügt also, $\sphericalangle PO_1X = \sphericalangle PO_2X'$ zu zeigen. Nach dem Zentri-Peripheriewinkelsatz gilt nun $\sphericalangle PO_1X = 2\sphericalangle PQX$ und $\sphericalangle X'O_2P = 2\sphericalangle X'QP$. Also ist

$$\sphericalangle PO_2X' = 360^\circ - \sphericalangle X'O_2P = 2(180^\circ - \sphericalangle X'QP) = 2\sphericalangle PQX = \sphericalangle PO_1X,$$

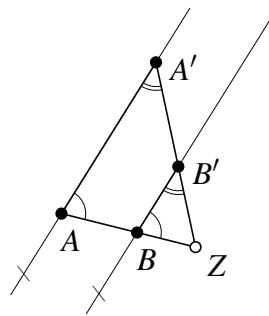
wie gewünscht. □

Beweis der Klassifikation. Offensichtlich sind Drehstreckungen und Verschiebungen orientierungserhaltende Ähnlichkeitsabbildungen. Sei umgekehrt σ eine orientierungserhaltende Ähnlichkeitsabbildung. Wähle zwei verschiedene Punkte A und B sowie ihre Bildpunkte $A' := \sigma(A)$ und $B' := \sigma(B)$. Für jeden weiteren Punkt X ist der Bildpunkt $X' := \sigma(X)$ eindeutig dadurch bestimmt, dass die Dreiecke ABX und $A'B'X'$ gleichsinnig ähnlich sein müssen. Es genügt also zu zeigen, dass stets eine Drehstreckung oder eine Verschiebung σ' existiert, die A auf A' und B auf B' abbildet. Denn aus der eben festgestellten Eindeutigkeit folgt dann auch $\sigma(X) = \sigma'(X)$ für jeden weiteren Punkt X , sodass zwangsläufig $\sigma = \sigma'$ ist.

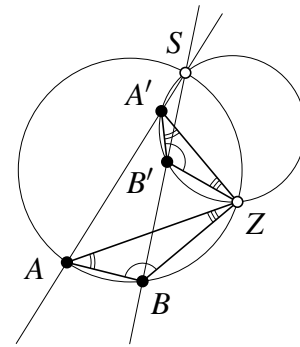
Um σ' zu konstruieren, unterscheiden wir (in aufsteigender Allgemeinheit) drei Fälle:



Fall 1



Fall 2



Fall 3

Fall 1: Es gilt $AA' \parallel BB'$ und $AB \parallel A'B'$. In diesem Fall ist $ABB'A'$ ein Parallelogramm und wir können σ' als diejenige Verschiebung wählen, die \overline{AB} auf $\overline{A'B'}$ abbildet.

Fall 2: Es gilt $AA' \parallel BB'$, aber $AB \not\parallel A'B'$. In diesem Fall sei Z der Schnittpunkt von AB und $A'B'$. Sei σ' die Drehstreckung mit Zentrum Z , die A auf A' abbildet. Nach dem Strahlensatz sind die Dreiecke $AA'Z$ und $BB'Z$ gleichsinnig ähnlich, weshalb σ' auch B auf B' abbildet.

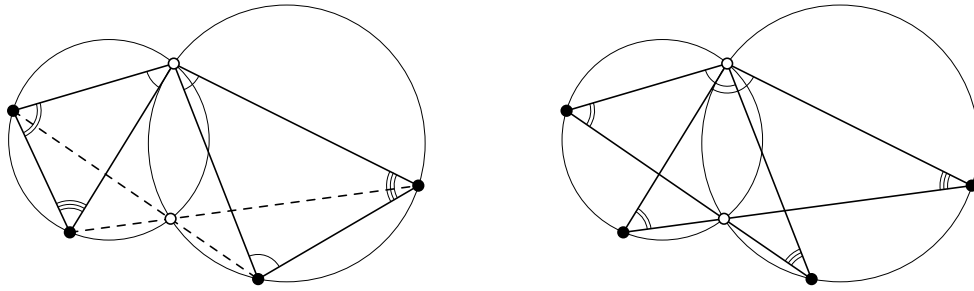
Fall 3: Es gilt $AA' \not\parallel BB'$. Sei S der Schnittpunkt von AA' und BB' und sei Z der zweite Schnittpunkt der Umkreise $\odot ABS$ und $\odot A'B'S$ (falls sich die Umkreise in S tangieren, wählen wir $Z = S$). Sei σ' die Drehstreckung mit Zentrum Z , die Kreis $\odot ABSZ$ auf den Kreis $\odot A'B'SZ$ abbildet. Aus dem Lemma folgt dann direkt, dass σ' den Punkt A auf A' und den Punkt B auf B' abbildet, wie gewünscht.

Damit ist gezeigt, dass jede orientierungserhaltende Ähnlichkeitsabbildung eine Drehstreckung oder eine Verschiebung ist. Die weiteren Behauptungen (a) und (b) sind nun einfache Folgerungen: Wenn σ_1 und σ_2 Drehstreckungen sind, dann ist die Hintereinanderausführung $\sigma_2 \circ \sigma_1$ offensichtlich wieder eine orientierungserhaltende Ähnlichkeitsabbildung, also eine Drehstreckung oder eine Verschiebung. Damit ist Behauptung (a) gezeigt.

Für Behauptung (b) betrachte den Fall, dass σ_1 und σ_2 Streckungen sind. Wir wissen schon, dass $\sigma_2 \circ \sigma_1$ eine Drehstreckung oder eine Verschiebung sein muss. Wenn wir eine Verschiebung vorliegen haben, sind wir fertig. Wir nehmen also an, dass $\sigma_2 \circ \sigma_1$ eine Drehstreckung ist. Streckungen schicken aber Geraden auf parallele Geraden. Für jede Gerade ℓ ist demzufolge $\ell \parallel \sigma_1(\ell) \parallel \sigma_2(\sigma_1(\ell))$. Der Drehwinkel von $\sigma_2 \circ \sigma_1$ muss also 0° oder 180° sein und somit haben wir es in der Tat mit einer Streckung (möglicherweise mit negativem Streckfaktor) zu tun.

Für Behauptung (c) betrachte den Fall, dass σ_1 und σ_2 Streckungen sind. Wir wissen schon, dass $\sigma_2 \circ \sigma_1$ eine Drehstreckung oder eine Verschiebung sein muss. Bei einer Verschiebung sind wir fertig. Andererseits ist klar, dass sich der Streckfaktor bei Hintereinanderausführung multipliziert. Wenn $\sigma_2 \circ \sigma_1$ eine Drehstreckung ist, muss der Streckfaktor folglich gleich 1 sein, sodass $\sigma_2 \circ \sigma_1$ eine Drehung ist. \square

Wie bereits erwähnt, ist das Lemma, das wir zum Beweis des Satzes benutzt haben, auch für sich genommen sehr nützlich. Zum Beispiel erhalten wir sofort die folgenden Paare ähnlicher Dreiecke:



In jedem Fall solltet ihr euch folgende Strategie merken:

Wenn sich in einer Aufgabe zwei Kreise schneiden, dann schaut euch die Drehstreckung um einen der beiden Schnittpunkte an, die den einen Kreis auf den anderen Kreis abbildet! Diese Drehstreckung kann auch als Projektion durch den anderen Schnittpunkt beschrieben werden.

Wenn ihr diese Strategie verinnerlicht habt, dann könnt ihr euch die obigen Ähnlichkeiten immer wieder herleiten, ganz egal, ob ihr ein Auge für solche Konfigurationen habt oder nicht.

Bearbeitet an dieser Stelle die folgenden beiden Beispielaufgaben. Wie üblich findet ihr am Ende des Kapitels Tipps und am Ende des Heftes Lösungen zu diesen Aufgaben.

Aufgabe 1. Sei $ABCD$ ein konvexes Viereck mit $|BC| = |DA|$. Auf den Seiten \overline{BC} und \overline{DA} liegen Punkte E und F mit $|BE| = |DF|$. Die Geraden AC und BD schneiden sich in P , die Geraden AC und EF schneiden sich in Q und die Geraden BD und EF schneiden sich in R . Die Umkreise $\odot BCP$ und $\odot DAP$ schneiden sich außer in P noch zusätzlich in S .

- Zeige, dass $BERS$, $CEQS$, $DFRS$ und $AFQS$ Sehnenvierecke sind.
- Zeige, dass $PQRS$ ein Sehnenviereck ist.

Aufgabe 2. Sei ABC ein Dreieck. Auf die Seiten \overline{BC} , \overline{CA} und \overline{AB} werden nach außen gleichseitige Dreiecke BXC , CYA und AZB aufgesetzt.

- Beweise, dass sich die Umkreise $\odot BXC$, $\odot CYA$ und $\odot AZB$ in einem Punkt P schneiden.
- Beweise, dass die Geraden AX , BY und CZ sich ebenfalls in P schneiden.

Aufgesetzte Dreiecke

Es gibt einen Typ von Aufgaben, in denen auf die Seiten eines Dreiecks weitere Dreiecke aufgesetzt werden; zu zeigen ist üblicherweise, dass das Dreieck, das von den Spitzen der aufgesetzten Dreiecke gebildet wird, eine bestimmte Eigenschaft hat. Beispiele für diesen Aufgabentyp sind Aufgabe 3, Aufgabe 4 und der Satz von Napoleon:

Aufgabe 3. Sei ABC ein Dreieck. Auf die Seiten \overline{CA} und \overline{AB} werden nach außen gleichschenklighrechtwinklige Dreiecke YCA mit Basis \overline{CA} und ZAB mit Basis \overline{AB} aufgesetzt. Sei M der Mittelpunkt von \overline{BC} . Zeige, dass das Dreieck MYZ gleichschenklighrechtwinklig ist.

Aufgabe 4. Sei ABC ein Dreieck. Auf die Seiten \overline{BC} , \overline{CA} und \overline{AB} werden nach außen Dreiecke BXC , CYA und AZB aufgesetzt. Dabei gelte $\sphericalangle XBC = \sphericalangle BCX = 15^\circ$, $\sphericalangle YCA = \sphericalangle ABZ = 45^\circ$ und $\sphericalangle CAY = \sphericalangle ZAB = 30^\circ$. Zeige, dass das Dreieck XYZ gleichschenklighrechtwinklig ist.

Satz von Napoleon. Sei ABC ein Dreieck. Auf die Seiten \overline{BC} , \overline{CA} und \overline{AB} werden nach außen gleichseitige Dreiecke XBC , YCA und ZAB aufgesetzt. Sei A_1 der Mittelpunkt von XBC , B_1 der Mittelpunkt von YCA und C_1 der Mittelpunkt von ZAB . Dann ist $A_1B_1C_1$ ebenfalls ein gleichseitiges Dreieck.

Diese Aufgaben lassen sich allesamt mithilfe von Drehstreckungen lösen.⁷ Allerdings sind diese Lösungen alles andere als offensichtlich. Am Ende dieses Kapitels findet ihr Tipps zu den Aufgaben und am Ende des Heftes könnt ihr die Lösungen nachlesen.

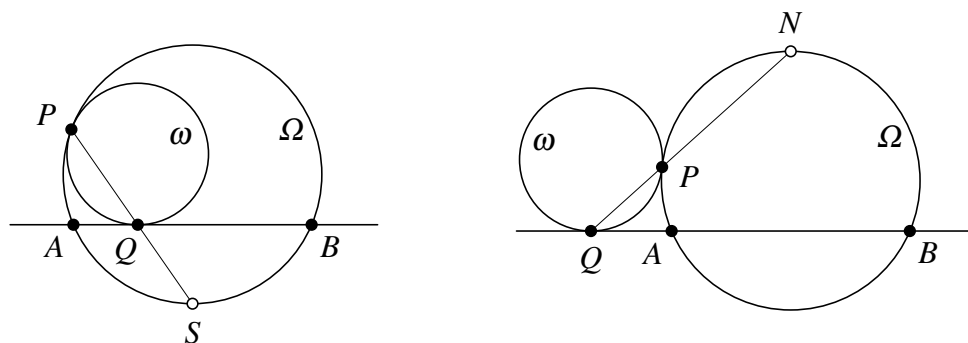
Streckungen und Kreise

Eine Streckung mit Zentrum Z bildet jeden Punkt X auf einen Punkt X' ab, sodass Z , X und X' auf einer Geraden liegen. Aus dieser trivialen Beobachtung ergeben sich viele nicht-triviale Folgerungen, wovon wir euch einige in diesem Unterkapitel nahebringen wollen.

Wir beginnen mit dem Kreisberührungslemma, das euch schon als Übungsaufgabe zur Inversion am Kreis im Heft für Klasse 9 begegnet ist. Es wird euch also wenig überraschen, dass das Kreisberührungslemma auch einen sehr eleganten Beweis mit Inversion zulässt (und wenn ihr diese Aufgabe noch nicht bearbeitet habt, sei sie euch ausdrücklich ans Herz gelegt).

Kreisberührungslemma. Sei Ω ein Kreis und A, B zwei Punkte auf Ω . Der Kreis ω berühre Ω in P und die Gerade AB in Q . Schließlich bezeichnen wir mit S und N die Bogenmittelpunkte der beiden Bögen \widehat{AB} von Ω , sodass N auf der gleichen Seite von AB wie ω liegt und S auf der anderen Seite.

- (a) Wenn ω den Kreis Ω von innen berührt, dann verläuft die Gerade PQ durch S . Wenn sich die Kreise von außen berühren, verläuft PQ durch N .
- (b) Wenn ω den Kreis Ω von innen berühren, gilt $|SP| \cdot |SQ| = |SA|^2$. Wenn sich die Kreise von außen berühren, gilt $|NP| \cdot |NQ| = |NA|^2$.



Beweis. Wir nehmen an, dass sich ω und Ω von innen berühren; der andere Fall geht analog. Sei σ die Streckung mit Zentrum P , die ω auf Ω abbildet. Dann ist $\sigma(AB)$ eine Tangente an Ω . Außerdem ist $\sigma(AB)$ parallel zu AB . Es gibt aber nur zwei Tangenten an Ω , die parallel zu AB sind, nämlich die Tangenten in S und N . Es gilt also $\sigma(Q) = S$ oder $\sigma(Q) = N$. Weil ω den Kreis Ω von innen berührt, muss σ einen Streckfaktor größer 1 haben. Also liegt $\sigma(Q)$ auf der Verlängerung von \overline{PQ} über Q hinaus. Folglich kommt nur $\sigma(Q) = S$ in Frage und wir erhalten, dass S auf der Geraden PQ liegt. Damit ist Behauptung (a) gezeigt.

Die Behauptung (b) lässt sich mithilfe ähnlicher Dreiecke beweisen: Weil S der Bogenmittelpunkt von \widehat{AB} ist, muss das Dreieck ABS gleichschenkelig sein und es gilt $\sphericalangle SAB = \sphericalangle ABS$. Nach dem Peripheriewinkelsatz gilt $\sphericalangle ABS = \sphericalangle APS$. Es folgt also $\sphericalangle SAQ = \sphericalangle APS$. Weil die Dreiecke ASQ

⁷Aufgabe 3 hat auch eine recht einfache Lösung mit kongruenten Dreiecken.

und ASP außerdem den Winkel $\sphericalangle QSA = \sphericalangle PSA$ gemeinsam haben, sind sie ähnlich. Es folgt $|SA|/|SQ| = |SP|/|SA|$ bzw. nach Umstellen $|SP| \cdot |SQ| = |SA|^2$, wie behauptet. \square

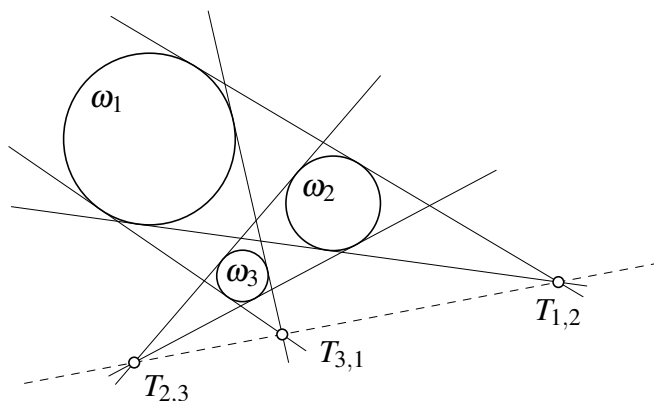
Im Kapitel zur Inversion aus dem Heft für Klasse 9 habt ihr gelernt, dass ihr, wann immer sich zwei Kreise berühren, am Berührungspunkt (oder einem anderen Punkt auf einem der beiden Kreise) invertieren solltet. Dieser Strategie stellen wir nun eine weitere zur Seite:

Wenn sich in einer Aufgabe zwei Kreise berühren, dann betrachtet die Streckung am Berührungspunkt, die den einen Kreis auf den anderen abbildet!

Auch wenn sich zwei Kreise nicht berühren, kann es sehr nützlich sein, den einen Kreis auf den anderen zu strecken. Auf diese Weise erhalten wir zum Beispiel einen sehr eleganten Beweis des folgenden Satzes:

Satz von Monge. Seien ω_1 , ω_2 und ω_3 drei Kreise. Wir nehmen an, dass die Radien der Kreise paarweise verschieden sind und dass keiner der drei Kreise innerhalb eines der anderen beiden Kreise liegt. Die äußeren gemeinsamen Tangenten von ω_1 und ω_2 schneiden sich in $T_{1,2}$, die äußeren gemeinsamen Tangenten von ω_2 und ω_3 schneiden sich in $T_{2,3}$ und die äußeren gemeinsamen Tangenten von ω_3 und ω_1 schneiden sich in $T_{3,1}$. Dann sind $T_{1,2}$, $T_{2,3}$ und $T_{3,1}$ kollinear.

Eine analoge Aussage gilt, wenn wir nur für ω_1 und ω_2 den Schnittpunkt der äußeren gemeinsamen Tangenten betrachten und für die anderen beiden Paare von Kreisen jeweils den Schnittpunkt der inneren gemeinsamen Tangenten (vorausgesetzt, die Kreise liegen so, dass die inneren gemeinsamen Tangenten existieren).



Beweis. Seien r_1 , r_2 und r_3 die Radien von ω_1 , ω_2 und ω_3 . Sei $\sigma_{1,2}$ die Streckung mit Zentrum $T_{1,2}$ und Faktor r_2/r_1 , die ω_1 auf ω_2 abbildet. Analog sei $\sigma_{2,3}$ die Streckung mit Zentrum $T_{2,3}$ und Faktor r_3/r_2 , die ω_2 auf ω_3 abbildet. Wir haben im vorherigen Unterkapitel gesehen, dass die Hintereinanderausführung $\sigma_{2,3} \circ \sigma_{1,2}$ wieder eine zentrische Streckung oder eine Verschiebung ist. Außerdem bildet $\sigma_{2,3} \circ \sigma_{1,2}$ den Kreis ω_1 auf den Kreis ω_3 ab. Nach Annahme haben ω_1 und ω_3 verschiedene Radien, also kann $\sigma_{2,3} \circ \sigma_{1,2}$ keine Verschiebung sein. Es kommt also nur eine Streckung in Frage. Weil sich Streckfaktoren bei Hintereinanderausführung multiplizieren, hat $\sigma_{2,3} \circ \sigma_{1,2}$ den Streckfaktor $r_2/r_1 \cdot r_3/r_2 = r_3/r_1 > 0$. Es gibt aber nur eine Streckung mit positivem Streckfaktor, die ω_1 auf ω_3 abbildet, nämlich die Streckung mit Zentrum $T_{3,1}$ und Faktor r_3/r_1 . Also muss $T_{3,1}$ das Zentrum von $\sigma_{2,3} \circ \sigma_{1,2}$ sein.

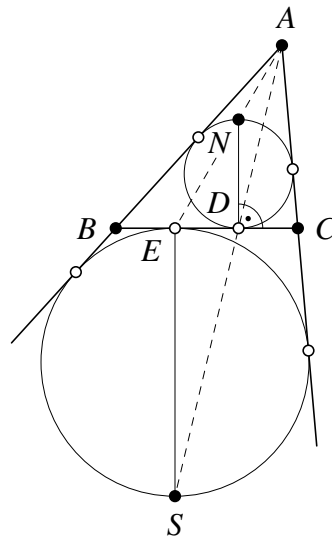
Andererseits bilden sowohl $\sigma_{1,2}$ als auch $\sigma_{2,3}$ die Gerade $T_{1,2}T_{2,3}$ auf sich selbst ab. Also muss auch $\sigma_{2,3} \circ \sigma_{1,2}$ die Gerade $T_{1,2}T_{2,3}$ auf sich selbst abbilden. Dann muss aber das Streckzentrum von $\sigma_{2,3} \circ \sigma_{1,2}$ auf $T_{1,2}T_{2,3}$ liegen. Das ist genau die Aussage, die wir zeigen wollten.

Die analoge Aussage folgt (wenig überraschend) analog, indem wir bemerken, dass es genau eine Streckung mit negativem Streckfaktor gibt, die ω_1 auf ω_3 abbildet, und dass das Zentrum dieser Streckung der Schnittpunkt der gemeinsamen inneren Tangenten von ω_1 und ω_3 ist. \square

Merkt euch nicht (nur) die Aussage des Satzes von Monge, sondern merkt euch vor allem den Beweis! Der Satz von Monge wird häufig in Spezialfällen angewendet, die nicht sofort als solche zu erkennen sind (zum Beispiel, wenn in einer Aufgabe viele Inkreise vorkommen). Es wird euch leichter fallen, wenn ihr euch die konkreten Streckungen in einem Spezialfall anschaut und damit den Satz von Monge für diesen Spezialfall erneut beweist.

Weitere Beispielaufgaben

Aufgabe 5. Sei ABC ein Dreieck. Der Inkreis ω berühre die Strecke \overline{BC} in D und der Ankreis ω_a gegenüber A berühre die Strecke \overline{BC} in E . Sei N der Punkt auf ω , der D diametral gegenüber liegt, und sei S der Punkt auf ω_a , der E diametral gegenüber liegt. Zeige, dass A , D und S sowie A , E und N jeweils kollinear sind.



Aufgabe 6. Gegeben ist ein Halbkreis Ω mit Durchmesser \overline{AB} . Auf Ω liege ein Punkt C , der von A und B verschieden ist. Der Lotfußpunkt von C auf AB heiße D . Ein Kreis ω liege außerhalb des Dreiecks ADC und berühre gleichzeitig den Halbkreis Ω sowie die Strecken \overline{AB} und \overline{CD} . Der Berührungspunkt von ω mit \overline{AB} sei E . Zeige, dass die Strecken \overline{AC} und \overline{AE} gleich lang sind.

(Aufgabe 6 habt ihr schon als Übungsaufgabe zur Inversion im Heft für Klasse 9 gesehen. Wenn ihr euch die Inversionslösung noch nicht überlegt habt, solltet ihr das nachholen.)

Aufgabe 7. Sei $ABCD$ ein konvexes Sehnenviereck mit Umkreis Ω und Umkreismittelpunkt O . Wir nehmen an, dass $|AC| \neq |BD|$. Die Diagonalen AC und BD schneiden sich in E . Eine Gerade ℓ durch O schneide die Strecken \overline{BE} und \overline{CE} in Punkten P und Q , sodass $|EP| = |EQ|$ gilt. Ein Kreis ω berühre die Strecken \overline{AE} und \overline{BE} und außerdem den Kreis Ω ; sei F der Berührungspunkt mit Ω . Die Geraden EF und ℓ schneiden sich in M . Beweise, dass die durch M gezogene Parallele zu AC den Kreis Ω berührt.

Tipps zu den Beispielaufgaben

Tipps zu Aufgabe 1. Um (a) zu zeigen, betrachte die Drehstreckung σ mit Zentrum S , die den Umkreis $\odot BCP$ auf den Umkreis $\odot DAP$ abbildet. Was kannst du über σ aussagen? Wiederhole dann das gleiche Argument mit \overline{BE} und \overline{DF} statt \overline{BC} und \overline{DA} .

Für (b) benutze (a) und eine Winkeljagd.

Tipps zu Aufgabe 2. Für (a) benutze eine Winkeljagd.

Um in (b) zu zeigen, dass sich BY und CZ in P schneiden, betrachte eine geeignete Drehstreckung mit Zentrum A .

Tipps zu Aufgabe 3. Betrachte die Drehstreckung σ mit Zentrum Z , Drehwinkel 45° und Faktor $\sqrt{2}$. Welchen Punkt bildet σ auf A ab? Zeige dann, dass $\sigma(M) = Y$.

Tipps zu Aufgabe 4. Betrachte die Drehstreckung σ mit Zentrum Z , Drehwinkel 45° und Faktor $\sqrt{2}$. Welchen Punkt bildet σ auf A ab? Zeige dann, dass $\sigma(X) = Y$.

Tipps zu Aufgabe 5. Betrachte die Streckung mit Zentrum A , die den Inkreis ω auf den Ankreis ω_a schickt.

Tipps zu Aufgabe 6. Benutze das Kreisberührungslemma.




Tipps zu Aufgabe 7. Wie muss ℓ liegen, damit die Bedingung $|EP| = |EQ|$ erfüllt ist?

Betrachte die Streckung mit Zentrum F , die ω auf Ω abbildet. Untersuche, worauf σ den Punkt E und die Gerade AC abbildet.

6 Geometrieaufgaben durchrechnen

Wenn ihr bei einer Geometrieaufgabe stecken bleibt, drängt sich früher oder später unweigerlich der Gedanke auf, ob sich die Aufgabe nicht einfach durchrechnen ließe. In diesem Abschnitt wollen wir besprechen, wie ihr damit erfolgreich sein könnt und was ihr vermeiden solltet.

Einige Warnungen vorweg. Ihr solltet euch folgender Dinge bewusst sein:

-  Durchrechnen ist nicht gern gesehen. Unvollständige Durchrechnenlösungen werden in der Regel sehr hart bewertet. Bei der IMO ist es sogar so streng, dass unvollständige Durchrechnenlösungen überhaupt keine Punkte bekommen. Lediglich Zwischenergebnisse, die zurück in die Sprache der Geometrie übersetzt wurden, werden honoriert.
-  Durchrechnen ist fehleranfällig. Die Korrekturerfahrung zeigt, dass die meisten Durchrechnenversuche an Umformungsfehlern scheitern. Je nachdem, wie früh ein solcher Fehler passiert, kann er sich auf fatale Weise fortpflanzen und seitenlange Rechnungen wertlos machen. Selbst bei weniger strengen Wettbewerben als der IMO werden solche Abgaben in der Regel mit sehr bescheidenen Punktzahlen bedacht.
-  Durchrechnen ist zeitaufwendig, besonders dann, wenn ihr merkt, dass ihr euch verrechnet habt, und ihr den Fehler suchen müsst.

Deswegen solltet ihr die folgenden Ratschläge beachten:

- Fangt nur an, eine Aufgabe durchzurechnen, wenn ihr euch einigermaßen sicher seid, dass ihr durchkommt.
- Macht euch vorher einen Plan: Welche Punkte sind am schwierigsten zu berechnen? Welche Annahmen und Vereinfachungen könnt ihr treffen, um die schwierigsten Schritte so einfach wie möglich zu machen?
- Versucht die Aufgabe immer zuerst elementar zu lösen. Denn selbst, wenn ihr euch später entschließt, die Aufgabe durchzurechnen, gibt es häufig einfache elementare Beobachtungen, die euch das Durchrechnen wesentlich erleichtern. Und wenn ihr beim Durchrechnen doch nicht erfolgreich seid, kriegt ihr für die elementaren Beobachtungen immerhin noch ein paar Punkte.

In meiner Erfahrung gibt es drei sinnvolle Methoden, Aufgaben durchzurechnen: Trigonometrie, komplexe Zahlen und baryzentrische Koordinaten. Cartesische Koordinaten, wie in der Schule, solltet ihr nur im absoluten Notfall verwenden, denn fast immer ist eine der anderen Methoden besser geeignet. Wir werden nun (kurz) das Durchrechnen mit Trigonometrie und mit komplexen Zahlen besprechen. Für baryzentrische Koordinaten gibt es zum Beispiel das sehr umfangreiche Skript *Barycentric Coordinates in Olympiad Geometry* von Max Schindler und Evan Chen⁸. Und zu komplexen Zahlen gibt es natürlich das berühmte Skript von Eric Müller.⁹

Durchrechnen mit Trigonometrie

Die Idee hierbei ist simpel: Ihr führt einige Winkel und Streckenlängen ein und rechnet dann alle weiteren Winkel durch Winkeljagd sowie alle weiteren Längen durch den Sinus- und den Cosinussatz aus (auch die Sätze von Ceva und Menelaos sind häufig mit von der Partie; allgemein sind solche Lösungen häufig ein Mix aus elementaren Argumenten und trigonometrischen Rechnungen). Trigonometrisches Durchrechnen hat den Vorteil, dass unvollständige Lösungen

⁸Online verfügbar unter <https://web.evanchen.cc/handouts/bary/bary-full.pdf>

⁹Dem Autoren ist leider nicht bekannt, ob dieses online verfügbar ist.

weniger hart bewertet werden, weil trigonometrische Längenbeziehungen eher für nützlich erachtet werden als korrekt ausgerechnete Koordinaten.

Beim trigonometrischen Durchrechnen gilt folgende Faustregel: *Der Sinussatz ist euer Freund, der Cosinussatz ist euer Feind.* Denn durch den Sinussatz bekommt ihr nur einige Faktoren hinzu, während der Cosinussatz mit Summen und Wurzeln daherkommt, die euch beim Ausmultiplizieren Kopfschmerzen bereiten werden. Natürlich lässt es sich oftmals nicht vermeiden, auch den Cosinussatz zu verwenden, aber ihr seid besser beraten, wenn ihr das Durchrechnen so strukturiert, dass der Cosinussatz möglichst wenig bzw. nur im letzten Schritt verwendet wird.

Ihr solltet es vermeiden, unbekannte Winkel durch arcsin oder arccos auszudrücken (es sei denn, ihr wollt zeigen, dass es sich etwa um einen 30° - oder 60° -Winkel handelt). Versucht lieber, direkt mit Sinus oder Cosinus des betreffenden Winkels zu arbeiten.

Um trigonometrisch erfolgreich zu sein, solltet ihr selbstverständlich die Additionstheoreme im Schlaf beherrschen. Ferner solltet ihr folgende Formeln kennen (oder zumindest wissen, dass sie existieren, und sie euch herleiten können):

Summe-zu-Produkt-Formeln. Für beliebige Winkel α und β gilt

$$\begin{aligned}\sin \alpha + \sin \beta &= 2 \sin\left(\frac{\alpha+\beta}{2}\right) \cos\left(\frac{\alpha-\beta}{2}\right), & \sin \alpha - \sin \beta &= 2 \cos\left(\frac{\alpha+\beta}{2}\right) \sin\left(\frac{\alpha-\beta}{2}\right), \\ \cos \alpha + \cos \beta &= 2 \cos\left(\frac{\alpha+\beta}{2}\right) \cos\left(\frac{\alpha-\beta}{2}\right), & \cos \alpha - \cos \beta &= -2 \sin\left(\frac{\alpha+\beta}{2}\right) \sin\left(\frac{\alpha-\beta}{2}\right).\end{aligned}$$

Trigonometrische Lösungen enden häufig damit, dass ihr eine trigonometrische Identität nachweisen müsst. Dafür ist es neben den obigen Formeln sehr nützlich, einige Beziehungen im Dreieck zu kennen. Im Folgenden bezeichnen a, b, c sowie α, β, γ stets die Seitenlängen und Winkelgrößen eines Dreiecks ABC . Wir beginnen mit einer erweiterten Form des Sinussatzes, die euch die Schule wahrscheinlich (leider) nicht so beigebracht hat.

Erweiterter Sinussatz. Wenn R der Umkreisradius von ABC ist, dann gilt

$$\frac{a}{\sin \alpha} = \frac{b}{\sin \beta} = \frac{c}{\sin \gamma} = 2R.$$

Aufgabe 1. Beweise die Summe-zu-Produkt-Formeln und den erweiterten Sinussatz!

Als nächstes haben wir die folgenden Formeln, die dem Autoren dieses Textes in seiner eigenen Olympiadezeit gute Dienste geleistet hat:

Halbwinkelformel. Sei $s := \frac{1}{2}(a+b+c)$ der halbe Umfang von ABC . Dann gilt

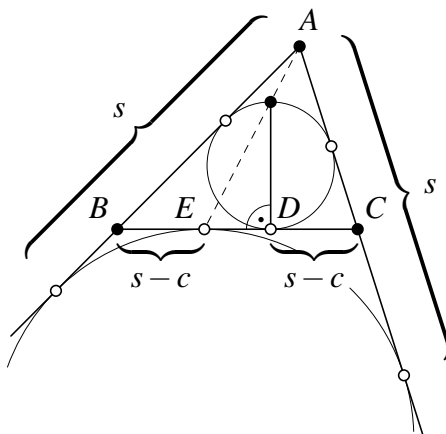
$$\sin\left(\frac{\alpha}{2}\right) = \sqrt{\frac{(s-b)(s-c)}{bc}} \quad \text{und} \quad \cos\left(\frac{\alpha}{2}\right) = \sqrt{\frac{s(s-a)}{bc}}.$$

Beweis. Nach Cosinussatz ist $\cos \alpha = (b^2 + c^2 - a^2)/(2bc)$. Damit folgen beide Behauptungen nach kurzem Umformen aus den für $0 \leq \alpha \leq 180^\circ$ gültigen Halbwinkelformeln

$$\sin\left(\frac{\alpha}{2}\right) = \sqrt{\frac{1 - \cos \alpha}{2}} \quad \text{und} \quad \cos\left(\frac{\alpha}{2}\right) = \sqrt{\frac{1 + \cos \alpha}{2}}. \quad \square$$

Die Halbwinkelformel ist nicht zuletzt deshalb nützlich, weil die Ausdrücke s und $s-a$ auf natürliche Weise im Dreieck ABC auftauchen.

Aufgabe 2. Beweise, dass die Ausdrücke s und $s-c$ als Tangentenabschnitte am In- und Ankreis auftreten, wie sie in der untenstehenden Skizze illustriert sind. Überlege dir auch die analogen Aussagen für $s-a$ und $s-b$.



Insbesondere ist der Tangentenabschnitt \overline{CD} am Inkreis genauso lang wie der Tangentenabschnitt \overline{BE} am Ankreis. Dieser Fakt kommt in Olympiadeaufgaben häufig vor und ihr solltet ihn euch merken. Zur Erinnerung ist in der Skizze außerdem der Fakt eingezeichnet, dass die Gerade durch A und den Ankreisberührpunkt E den Inkreis in dem Punkt schneidet, der dem Inkreisberührpunkt D gegenüber liegt (siehe Aufgabe 5 im Kapitel über Drehstreckungen).

Die Ausdrücke s und $s - a$, $s - b$, $s - c$ kommen noch in weiteren Formeln vor.

Satz von Heron. Der Flächeninhalt A eines Dreiecks ABC ist gegeben durch

$$A = \sqrt{s(s-a)(s-b)(s-c)}.$$

Beweis. Ausgehend von der trigonometrischen Flächeninhaltsformel $A = \frac{1}{2}bc \sin \alpha$ schreiben wir $\sin \alpha = 2 \sin\left(\frac{\alpha}{2}\right) \cos\left(\frac{\alpha}{2}\right)$ und setzen die Halbwinkelformeln ein. \square

Formeln für die In-, An- und Umkreisradien. Wie oben sei A der Flächeninhalt von ABC . Sei außerdem r der Inkreisradius, r_a der Radius des A gegenüberliegenden Ankreises und R der Umkreisradius. Dann gilt

$$r = \frac{A}{s}, \quad r_a = \frac{A}{s-a} \quad \text{und} \quad R = \frac{abc}{4A}.$$

Beweis. Sei I der Inkreismittelpunkt. Dann gilt $A = A_{BCI} + A_{CAI} + A_{ABI}$. Andererseits hat die Höhe von I auf die Seiten BC , CA und AB stets die Länge r . Es gilt also $A_{BCI} = \frac{1}{2}ar$, $A_{CAI} = \frac{1}{2}br$ und $A_{ABI} = \frac{1}{2}cr$. Also ist $A = \frac{1}{2}(a+b+c)r = sr$, woraus die Formel für den Inkreisradius r sofort folgt. Die Formel für r_a folgt aus einem ähnlichen Argument und ist eine gute Übungsaufgabe. Die Formel für R folgt schließlich aus dem erweiterten Sinussatz $a/\sin \alpha = 2R$ und der trigonometrischen Flächeninhaltsformel $A = \frac{1}{2}bc \sin \alpha$. \square

Um euch eine Idee zu geben, wie das Durchrechnen mit Seitenlängen und Trigonometrie aussehen kann, werden wir eine Lösung der folgenden, ziemlich schweren Aufgabe skizzieren. Es gibt natürlich (wie immer bei Durchrechnenlösungen) auch eine schöne Lösung. Findest du sie?

Aufgabe 3.** Sei ABC ein Dreieck. Der Ankreis ω_a gegenüber A berühre die Geraden BC , AC und AB in den Punkten D , E und F . Der Umkreis $\odot AEF$ schneide die Gerade BC in den Punkten P und Q . Schließlich sei M der Mittelpunkt der Strecke AD . Beweise, dass der Umkreis $\odot MPQ$ den Ankreis ω_a berührt.

Lösung. Wie bei jeder guten Durchrechnenlösung beginnen wir mit einigen elementaren Betrachtungen. Durch eine genaue Skizze vermuten wir, dass der Berührungspunkt auch auf der Geraden AD liegt. Also sei T der Schnittpunkt von AD mit ω_a . Sei Ω' der Kreis durch T und D , der ω_a tangiert und seien P' , Q' die Schnittpunkte von Ω' mit BC . Um die Behauptung zu zeigen,

einsetzen, erhalten wir

$$\begin{aligned}
 |PL|^2 &= |AN|^2 - |NL|^2 = \left(\frac{s}{2 \cos(\frac{\alpha}{2})} \right)^2 - \frac{h_a^2}{4} - \frac{r_a^2}{4} + \frac{r_a h_a}{2} \\
 &= \frac{s^2}{4} \cdot \frac{bc}{s(s-a)} - \frac{A^2}{a^2} - \frac{A^2}{4(s-a)^2} + \frac{A^2}{a(s-a)} \\
 &= \frac{s(a^2 bc - 4(s-a)^2(s-b)(s-c) - a^2(s-b)(s-c) + 4a(s-a)(s-b)(s-c))}{4a^2(s-a)}
 \end{aligned}$$

Hier haben wir nacheinander die Halbwinkelformel $\cos(\frac{\alpha}{2}) = (s(s-a))/(bc)$, die Flächeninhaltsformel $h_a = 2A/a$, die Formel $r_a = A/(s-a)$ sowie den Satz von Heron eingesetzt. Im letzten Schritt haben wir außerdem schon einmal $s-a$ gekürzt. Wegen $a^2 bc - a^2(s-b)(s-c) = a^2 s(s-a)$ lässt sich der Faktor $s-a$ ein weiteres mal kürzen und wir erhalten

$$|PL|^2 = \frac{s(a^2 s - 4(s-a)(s-b)(s-c) + 4a(s-b)(s-c))}{4a^2(s-a)}$$

Indem wir diesen Term mit dem Term für $|P'L|^2$ vergleichen, sehen wir, dass wir nur noch $a^2 s - (b-c)^2 s = 4(s-a)(s-b)(s-c) + 4a(s-b)(s-c)$ zeigen müssen. Das ist nun klar, denn beide Terme lassen sich unmittelbar zu $4s(s-b)(s-c)$ umformen. \square

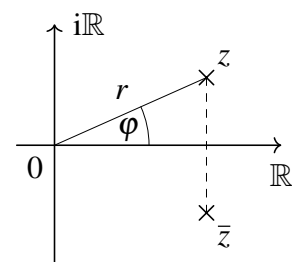
Komplex durchrechnen

Grundbegriffe. Die Menge der *komplexen Zahlen* \mathbb{C} entsteht, indem wir zu den reellen Zahlen \mathbb{R} eine *imaginäre Einheit* i hinzufügen, die $i^2 = -1$ erfüllt. Eine allgemeine komplexe Zahl ist dann durch $z = x + iy$ gegeben, wobei x und y reelle Zahlen sind.

Die komplexen Zahlen haben eine Reihe von Vorteilen gegenüber den reellen Zahlen. Zum Beispiel ist sofort klar, dass sich alle quadratischen Gleichungen in \mathbb{C} lösen lassen, denn das Hinzufügen von i erlaubt uns, auch Wurzeln aus negativen Zahlen zu ziehen. Tatsächlich gilt das nicht nur für quadratische Gleichungen: In \mathbb{C} lassen sich *alle* polynomiellen Gleichungen lösen, egal von welchem Grad!¹⁰ Dieser Fakt wird auch als *Fundamentalsatz der Algebra* bezeichnet. Einen Beweis für die werdet ihr im Studium sehen; er würde hier zu weit führen.

Wir wollen in diesem Kapitel erklären, wie sich komplexe Zahlen in der Geometrie verwenden lassen. Die Grundidee ist folgende: Statt Punkte in der Ebene durch Koordinaten (x, y) zu beschreiben, können wir sie auch als komplexe Zahlen $z = x + iy$ auffassen. Die reellen Zahlen liegen dann auf der x -Achse, während die *rein imaginären* Zahlen, also die komplexen Zahlen der Form $0 + iy$, auf der y -Achse liegen. Deshalb werden wir im Folgenden stattdessen von der *reellen* und der *imaginären Achse* sprechen.

Der *Betrag* von z ist definiert als $|z| := \sqrt{x^2 + y^2}$, also als der Abstand zum Ursprung. Wenn $r = |z|$, dann können wir z auch in „Polarkoordinaten“ als $z = r(\cos \varphi + i \sin \varphi)$ schreiben, wobei φ der Winkel ist, den die Strecke von 0 nach z mit der reellen Achse einschließt. Wir nennen φ auch das *Argument* von z . Die komplexe Zahl $x - iy$, also das Spiegelbild von z an der reellen Achse, nennen wir die *zu z konjugierte komplexe Zahl*, und wir schreiben $\bar{z} := x - iy$.



Rechnen mit komplexen Zahlen. Wir können komplexe Zahlen wie gewohnt addieren, subtrahieren und multiplizieren. Nach der dritten

Betrag, Argument und Konjugiertes

¹⁰Diesen Fakt haben wir bereits in Kapitel 1: *Lineare Rekursionen* verwendet.

binomischen Formel gilt dann

$$z\bar{z} = (x + iy)(x - iy) = x^2 - i^2y^2 = x^2 + y^2 = |z|^2.$$

Diese Beobachtung erlaubt uns, auch durch komplexe Zahlen zu dividieren (außer durch 0 natürlich), denn wir können

$$\frac{z_1}{z_2} = \frac{1}{|z_2|^2} \cdot z_1 \bar{z}_2$$

schreiben (und $1/|z_2|^2$ ist schon definiert, denn $|z_2|$ ist ja eine reelle Zahl). Ihr könnt euch leicht überlegen, dass sich die komplexe Konjugation mit Addition, Subtraktion, Multiplikation und Division verträgt, das heißt es gilt

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2, \quad \overline{z_1 - z_2} = \bar{z}_1 - \bar{z}_2, \quad \overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2 \quad \text{und} \quad \overline{z_1/z_2} = \bar{z}_1/\bar{z}_2.$$

Multiplikation als Drehstreckung. Bei der Multiplikation von komplexen Zahlen in Polarkoordinaten ergibt sich nun etwas Interessantes: Wenn nämlich $z_1 = r_1(\cos \varphi_1 + i \sin \varphi_1)$ und $z_2 = r_2(\cos \varphi_2 + i \sin \varphi_2)$ ist, dann gilt

$$\begin{aligned} z_1 z_2 &= r_1 r_2 \left((\cos \varphi_1 \cos \varphi_2 - \sin \varphi_1 \sin \varphi_2) + i(\sin \varphi_1 \cos \varphi_2 + \cos \varphi_1 \sin \varphi_2) \right) \\ &= r_1 r_2 (\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2)), \end{aligned}$$

worin wir die Additionstheoreme für Sinus und Cosinus erkannt haben. Wenn wir also mit einer komplexen Zahl $z = r(\cos \varphi + i \sin \varphi)$ multiplizieren, dann multiplizieren wir den Betrag mit r und addieren φ zum Argument. Mit anderen Worten: *Multiplikation mit z ist eine Drehstreckung um den Punkt 0, mit Streckfaktor r und Drehwinkel φ !*

Geometrie mit komplexen Zahlen. Mithilfe dieser Beobachtung können wir effektiv Geometrie mit komplexen Zahlen betreiben. Betrachte zum Beispiel vier Punkte A, B, C und D in der Ebene. Seien a, b, c und d die entsprechenden komplexen Zahlen. Dann stehen die Geraden AB und CD genau dann senkrecht aufeinander, wenn die Drehstreckung, die durch Multiplikation mit der komplexen Zahl $z := (a - b)/(c - d)$ gegeben ist, den Winkel 90° oder 270° hat. Also gilt $AB \perp CD$ genau dann, wenn das Argument von z durch 90° oder 270° gegeben ist. Das wiederum ist äquivalent dazu, dass z rein imaginär ist, was wir mithilfe der komplexen Konjugation ein weiteres Mal zu $z = -\bar{z}$ äquivalent umformen können. Wir erhalten also, dass AB und CD genau dann senkrecht aufeinander stehen, wenn

$$\frac{a - b}{c - d} = -\frac{\bar{a} - \bar{b}}{\bar{c} - \bar{d}}$$

gilt. Eine ähnliche Überlegung verrät uns, dass AB und CD genau dann parallel sind, wenn $z := (a - b)/(c - d)$ das Argument 0° oder 180° hat. Das ist wiederum äquivalent dazu, dass z reell ist, was wir auch durch die Bedingung $z = \bar{z}$ ausdrücken können. Also sind AB und CD genau dann parallel, wenn

$$\frac{a - b}{c - d} = \frac{\bar{a} - \bar{b}}{\bar{c} - \bar{d}}.$$

Ein Punkt X liegt auf der Geraden AB genau dann, wenn AX und AB parallel sind. Mit den obigen Überlegungen ist das äquivalent zu der Gleichung

$$\frac{x - a}{b - a} = \frac{\bar{x} - \bar{a}}{\bar{b} - \bar{a}}.$$

Wir können also Geraden in komplexen Zahlen beschreiben.

Ähnlich verhält es sich mit Kreisen. Seien A, B, C und X vier Punkte in der Ebene und seien a, b, c und x die zugehörigen komplexen Zahlen. Wir nehmen der Einfachheit halber an, dass C und X in der gleichen Halbebene bezüglich AB liegen. Nach dem Peripheriewinkelsatz liegt X genau dann auf dem Umkreis $\odot ABC$, wenn $\sphericalangle AXB = \sphericalangle ACB$. Das ist genau dann der Fall, wenn die Drehstreckungen, die durch Multiplikation mit den komplexen Zahlen $z_1 := (a-x)/(b-x)$ und $z_2 := (a-c)/(b-c)$ gegeben sind, den gleichen Drehwinkel haben. Die komplexen Zahlen z_1 und z_2 müssen also das gleiche Argument haben. Das wiederum ist äquivalent dazu, dass z_1/z_2 das Argument 0° hat, also eine nichtnegative reelle Zahl ist. Wenn X und C in verschiedenen Halbebenen bezüglich AB liegen, erhalten wir analog die Bedingung, dass z_1/z_2 das Argument 180° hat, also eine nichtpositive reelle Zahl ist. Insgesamt sehen wir, dass X genau dann auf dem Umkreis $\odot ABC$ liegt, wenn z_1/z_2 reell ist, also genau dann, wenn

$$\frac{a-x}{b-x} \bigg/ \frac{a-c}{b-c} = \frac{\bar{a}-\bar{x}}{\bar{b}-\bar{x}} \bigg/ \frac{\bar{a}-\bar{c}}{\bar{b}-\bar{c}}.$$

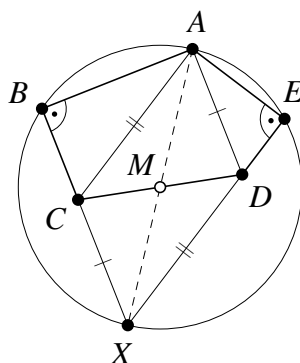
Aufgabe 4. Betrachte sechs Punkte A, B, C und A', B', C' . Seien a, b, c und a', b', c' die entsprechenden komplexen Zahlen. Zeige, dass die Dreiecke ABC und $A'B'C'$ genau dann gleichsinnig ähnlich sind, wenn folgendes gilt:

$$\frac{b-a}{c-a} = \frac{b'-a'}{c'-a'}.$$

Wir werden nun an einem Beispiel demonstrieren, wie sich Olympiadeaufgabe mit komplexen Zahlen durchrechnen lassen.

Aufgabe 5. Gegeben sei ein konvexes Fünfeck $ABCDE$ mit $\sphericalangle CBA = \sphericalangle AED = 90^\circ$. Der Mittelpunkt des Umkreises $\odot ABE$ sei M und der Mittelpunkt des Umkreises $\odot ACD$ sei O . Beweise: Wenn M der Mittelpunkt der Strecke \overline{CD} ist, dann verläuft die Gerade AO durch den Mittelpunkt der Strecke \overline{BE} .

Lösung. Wir beginnen zuerst mit einigen elementaren Beobachtungen (was, wie bereits erwähnt, immer eine gute Idee ist). Sei X der Schnittpunkt der Geraden BC und DE (diese können nicht parallel sein, sonst würde das Fünfeck bei A entarten). Wegen $\sphericalangle XBA = \sphericalangle AEX = 90^\circ$ ist \overline{AX} ein Durchmesser des Umkreises $\odot ABE$. Der Umkreismittelpunkt M muss also auch der Mittelpunkt von \overline{AX} sein. Das Viereck $ACXD$ muss also ein Parallelogramm sein, denn seine Diagonalen halbieren sich.



Nun rechnen wir komplex durch. Die zu A, B, \dots gehörigen komplexen Zahlen bezeichnen wir mit a, b, \dots . Ohne Einschränkung dürfen wir annehmen, dass $\odot ACD$ der komplexe Einheitskreis ist (es ist immer praktisch, einen geeigneten Kreis auf den Einheitskreis zu legen). Dann gilt $1 = |a|^2 = a\bar{a}$, also $\bar{a} = 1/a$. Analog folgt $\bar{c} = 1/c$ und $\bar{d} = 1/d$. Der Mittelpunkt des komplexen Einheitskreises ist 0, also gilt $O = 0$.

Weil B auf CX liegt und $ACXD$ ein Parallelogramm ist, müssen BC und AD parallel sein. Wir erhalten also

$$\frac{b-c}{d-a} = \frac{\bar{b}-\bar{c}}{\bar{d}-\bar{a}} \iff \bar{b}-\bar{c} = (b-c) \left(\frac{\bar{d}-\bar{a}}{d-a} \right) = -\frac{b-c}{ad}.$$

Im letzten Schritt haben wir $\bar{a} = 1/a$ und $\bar{d} = 1/d$ eingesetzt, um $(\bar{d}-\bar{a})/(d-a) = -1/(ad)$ zu erhalten. (Vereinfachungen von dieser Sorte sind einer der Gründe, warum es praktisch ist, möglichst viele Punkte auf den Einheitskreis zu legen.) Nach Voraussetzung ist ferner $AB \perp BC$. Wegen $AD \parallel BC$ muss auch $AB \perp AD$ sein. Wir erhalten also

$$\frac{a-b}{d-a} = -\frac{\bar{a}-\bar{b}}{\bar{d}-\bar{a}} \iff \bar{b}-\bar{a} = (a-b) \left(\frac{\bar{d}-\bar{a}}{d-a} \right) = -\frac{a-b}{ad},$$

wobei wir wieder $\bar{a} = 1/a$ und $\bar{d} = 1/d$ eingesetzt haben. Indem wir die Gleichungen für $\bar{b}-\bar{a}$ und $\bar{b}-\bar{c}$ voneinander subtrahieren, erhalten wir

$$\bar{c}-\bar{a} = \frac{2b-(a+c)}{ad} \iff b = \frac{a+c+ad(\bar{c}-\bar{a})}{2} = \frac{ac+c^2+ad-cd}{2c},$$

wobei wir im letzten Schritt $\bar{a} = 1/a$ und $\bar{c} = 1/c$ eingesetzt haben. Aus Symmetriegründen lässt sich e völlig analog berechnen; dabei werden lediglich die Rollen von c und d vertauscht. Wir erhalten also

$$e = \frac{ad+d^2+ac-cd}{2d}.$$

Der Mittelpunkt von \overline{BE} entspricht offensichtlich der komplexen Zahl $(b+e)/2$. Aus den Gleichungen für b und e folgt

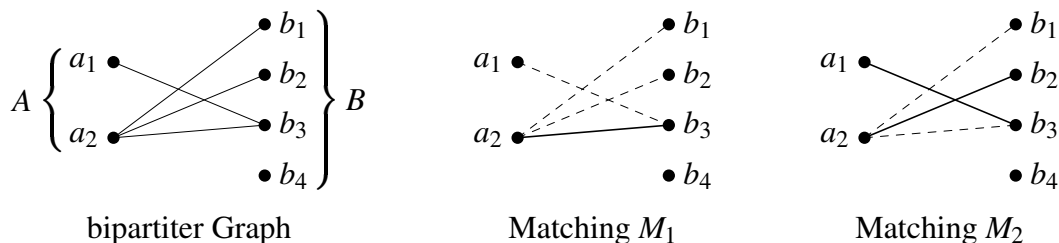
$$\frac{b+e}{2} = \frac{(ac+c^2+ad-cd)d + (ad+d^2+ac-cd)c}{4cd} = \frac{2acd+ad^2+ac^2}{4cd} = a \frac{(c+d)^2}{4cd}.$$

Um zu zeigen, dass A , O und der Mittelpunkt von \overline{BE} kollinear sind, können wir die allgemeine Bedingung verwenden und werden zweifellos nach kurzer Rechnung zum Ziel kommen. Wir können uns aber noch ein wenig schlauer anstellen: Wegen $O = 0$ müssen wir lediglich zeigen, dass $(b+e)/2$ ein reelles Vielfaches von a ist. Dank der Gleichung für $(b+e)/2$ müssen wir also nur zeigen, dass der Faktor $(c+d)^2/(4cd)$ eine reelle Zahl ist. Wegen $\bar{c} = 1/c$ und $\bar{d} = 1/d$ erhalten wir $\bar{c}+\bar{d} = (c+d)/(cd)$, also ist $(c+d)^2/(4cd) = \frac{1}{4}(c+d)(\bar{c}+\bar{d}) = \frac{1}{4}|c+d|^2$. Dieser Ausdruck ist definitiv eine reelle Zahl und wir sind fertig. \square

7 Der Heiratssatz

Lösungen von Kombinatorikaufgaben sind häufig lang und konfus, denn hier ist es viel schwieriger als zum Beispiel in Geometrie, eure Ideen in klare Formeln und Worte zu fassen. Dementsprechend häufig sind unvollständige Lösungen und Punktabzüge. An dieser Stelle kann häufig der *Heiratssatz* aushelfen und aus einem „Wurschtelargument“ eine saubere, wasserfeste Lösung machen, bzw. euch überhaupt erst auf eine vernünftige Lösung führen.

Bevor wir den Satz formulieren und beweisen können, müssen wir ein wenig Terminologie einführen. erinnert euch (siehe das Kapitel *Graphentheorie* im Heft für Klasse 9), dass ein *bipartiter Graph* ein Graph $G = (V, E)$ ist, dessen Knotenmenge $V = A \cup B$ sich in zwei disjunkte Teilmengen A und B zerlegen lässt, sodass Kanten nur zwischen A und B verlaufen, aber nicht innerhalb von A oder B . Ein *Matching* in einem bipartiten Graphen $G = (A \cup B, E)$ ist eine Teilmenge $M \subseteq E$ von Kanten, sodass M für jeden Knoten von G höchstens eine ausgehende Kante enthält. Die folgende Abbildung zeigt einen bipartiten Graphen G sowie zwei mögliche Matchings M_1 und M_2 in G .



Die Matchings M_1 und M_2 sind zugleich *inklusionsmaximale Matchings*: Würden wir nämlich noch irgendeine weitere Kante zu M_1 oder M_2 hinzufügen, dann würden mindestens zwei Kanten von einem der Knoten b_3 oder a_2 ausgehen und wir hätten kein Matching mehr.

Der *Heiratssatz* geht nun der Frage nach, für welche bipartiten Graphen $G = (A \cup B, E)$ ein Matching M existiert, das alle Knoten von A überdeckt. Für den obigen Graphen ist dies offenbar der Fall, denn M_2 ist genau ein solches Matching. Gleichzeitig zeigt das Beispiel, dass *nicht* jedes inklusionsmaximale Matching diese Bedingung erfüllt. Das Problem ist also nicht völlig trivial. Um den Heiratssatz formulieren zu können, müssen wir noch folgende Notation einführen: Für jede Teilmenge $S \subseteq A$ soll $N_G(S)$ die Menge aller Knoten aus B sein, die mit mindestens einem Knoten aus S durch eine Kante verbunden sind. Im obigen Beispiel ist etwa $N(\{a_1\}) = \{b_1, b_2, b_3\}$ und $N(A) = \{b_1, b_2, b_3\}$. Der Heiratssatz besagt nun Folgendes:

Heiratssatz. In einem bipartiten Graphen $G = (A \cup B, E)$ existiert genau dann ein Matching, das alle Knoten aus A überdeckt, wenn für jede Teilmenge $S \subseteq A$ die folgende Ungleichung erfüllt ist:

$$|N_G(S)| \geq |S|.$$

Der Name *Heiratssatz* hat folgenden altväterlichen Ursprung: Klassischerweise stellt man sich A und B als Mengen von Frauen bzw. Männern vor, wobei möglichst alle Frauen verheiratet werden sollen; die Menge E der Kanten gibt dabei die „akzeptablen“ Paarungen vor. Der entstehende Graph ist bipartit, weil „damals“ (in Deutschland vor 2017) Hochzeiten zwischen gleichgeschlechtlichen Paaren nicht „akzeptabel“ waren.

Wir werden gelegentlich davon sprechen, zwei Knoten $a \in A$ und $b \in B$ zu „verheiraten“, wenn wir ein Matching konstruieren, das die Kante ab enthält.

Es gibt viele Beweise für den Heiratssatz und Verallgemeinerungen des Problems führen in das faszinierende Feld der *Flussprobleme*. Hier werden wir stattdessen einen sehr einfachen Beweis per Induktion präsentieren.

Beweis. Wir nehmen zunächst an, dass ein Matching M existiert, das alle Knoten aus A enthält. Sei $S \subseteq A$ eine nichtleere Teilmenge. Jeder Knoten $s \in S$ ist Ausgangsknoten einer Kante $st \in M$. Die Endknoten t liegen in $N_G(S)$ und sind nach Definition eines Matchings paarweise verschieden. Es folgt sofort $|N_G(S)| \geq |S|$, wie behauptet.

Der schwierige Teil ist also die Rückrichtung. Wir benutzen Induktion über $|A|$. Der Fall $|A| = 1$ ist klar. Sei also $|A| > 1$ und wir dürfen annehmen, dass der Heiratssatz für Mengen mit weniger als $|A|$ Elementen gilt. Jetzt unterscheiden wir zwei Fälle.

Fall 1: Es gibt eine echte Teilmenge $S^* \subsetneq A$ für die $|N_G(S^*)| = |S^*|$ gilt. Wir können die Induktionsannahme auf S^* anwenden und erhalten ein Matching M^* , das alle Knoten von S^* überdeckt. Jetzt löschen wir alle Knoten aus S^* und $N_G(S^*)$ sowie alle Kanten, die von diesen Knoten ausgehen. Sei $\bar{G} = (\bar{A} \cup \bar{B}, \bar{E})$ der übrigbleibende bipartite Graph, wobei $\bar{A} = A \setminus S^*$ und $\bar{B} = B \setminus N_G(S^*)$. Für jede Teilmenge $T \subseteq \bar{A}$ gilt dann

$$|N_{\bar{G}}(T)| = |N_G(T \cup S^*) \setminus N_G(S^*)| = |N_G(T \cup S^*)| - |S^*| \geq |T \cup S^*| - |S^*| = |T|$$

Der Graph \bar{G} erfüllt also ebenfalls die fragliche Bedingung. Nach der Induktionsannahme enthält \bar{G} ein Matching \bar{M} , das alle Knoten von \bar{A} überdeckt. Dann ist $M := M^* \cup \bar{M}$ ein Matching in G , das alle Knoten von A überdeckt.

Fall 2: Für jede echte Teilmenge $S \subsetneq A$ gilt $|N_G(S)| \geq |S| + 1$. In diesem Fall wählen wir einfach irgendeine Kante ab und verheiraten die Knoten a und b . Danach löschen wir a und b sowie alle Kanten, die von einem der beiden Knoten ausgehen. Sei $\bar{G} = (\bar{A} \cup \bar{B}, \bar{E})$ der übrigbleibende bipartite Graph, wobei $\bar{A} = A \setminus \{a\}$ und $\bar{B} = B \setminus \{b\}$. Jede Teilmenge $S \subseteq \bar{A}$ ist eine echte Teilmenge von A und erfüllt somit $|N_G(S)| \geq |S| + 1$. Da in \bar{G} nur ein Knoten aus B entfernt wurde, gilt

$$|N_{\bar{G}}(S)| \geq |N_G(S)| - 1 \geq |S|.$$

Der Graph \bar{G} erfüllt also ebenfalls die fragliche Bedingung. Nach der Induktionsannahme enthält \bar{G} ein Matching \bar{M} , das alle Knoten von \bar{A} überdeckt. Dann ist $M := \{ab\} \cup \bar{M}$ ein Matching in G , das alle Knoten von A überdeckt. \square

Beispielaufgaben

Ihr sollt nun den Heiratssatz selbstständig auf mehrere Olympiadeaufgaben anwenden. Dazu müsst ihr euch zuerst überlegen, welche Objekte ihr überhaupt verheiraten wollt, sprich, ihr müsst die Aufgabe in geeigneter Weise in ein Matching-Problem übersetzen (das ist üblicherweise alles andere als offensichtlich). Danach müsst ihr nachweisen, dass die Bedingung aus dem Heiratssatz erfüllt ist.

Am Ende des Kapitels findet ihr Tipps und am Ende des Heftes findet ihr Lösungen zu den Beispielaufgaben. Ihr solltet zumindest versuchen, euch den ersten Teil jeder Lösung, also die Umformulierung in ein Matching-Problem, selber zu überlegen, damit ihr ein Gefühl bekommt, in welchen Situationen der Heiratssatz das Mittel der Wahl ist.

Aufgabe 1. Gegeben sind n^2 Kugeln in n verschiedenen Farben; von jeder Farbe gibt es genau n Kugeln. Diese Kugeln werden gleichmäßig auf n Schalen aufgeteilt, das heißt in jede Schale kommen genau n Kugeln. Zeige: Es ist stets möglich, aus jeder Schale eine Kugel auszuwählen, sodass die n ausgewählten Kugeln paarweise verschieden gefärbt sind!

Aufgabe 2. Tracey hat einen quadratischen Kuchen gebacken und in $n \times n$ kleine quadratische Stückchen aufgeteilt. Auf einigen Stückchen verteilt sie Erdbeeren (dabei dürfen Stückchen auch mehrere oder gar keine Erdbeeren erhalten), und zwar so, dass in jeder Zeile und jeder Spalte des Kuchens genau 2025 Erdbeeren liegen. Norman möchte nun heimlich ein paar der Erdbeeren

naschen. Damit Tracey möglichst nichts auffällt, sollen danach in jeder Zeile und jeder Spalte noch genau 2024 Erdbeeren liegen. Zeige, dass Norman das stets erreichen kann!

Aufgabe 3*. Gegeben seien positive ganze Zahlen n und N , sodass $N \geq n^{n-1}$. Beweise: Es existieren paarweise verschiedene Primzahlen p_1, \dots, p_n , sodass $p_i \mid N + i$ für alle $i = 1, 2, \dots, n$.

Wenn ihr Aufgabe 3 selbst lösen wollt, solltet ihr zuerst die folgende reine Zahlentheorie-Aufgabe lösen (diese ist absolut nicht einfach).

Aufgabe 4*. Für neun paarweise verschiedene positive ganze Zahlen d_1, d_2, \dots, d_9 betrachten wir das Polynom $P(X) := (X + d_1)(X + d_2) \cdots (X + d_9)$. Zeige, dass es eine positive ganze Zahl N gibt, sodass die ganze Zahl $P(n)$ für alle $n \geq N$ einen Primfaktor > 20 besitzt.

Aufgabe 5*. Gegeben sei ein quadratisches $3n \times 3n$ -Brett, dessen $9n^2$ Felder in drei verschiedenen Farben gefärbt sind. Dabei ist das Feld in der i -ten Zeile und j -ten Spalte in einer der Farben Azur, Bordeaux oder Citrin gefärbt, je nachdem, ob $i + j$ den Rest 0, 1 oder 2 modulo 3 lässt. Auf jedem Feld steht ein Spielstein. Diese Spielsteine sind ebenfalls in den drei Farben gefärbt, wobei es von jeder Farbe genau $3n^2$ Spielsteine gibt. Allerdings muss ein Spielstein zu Beginn nicht auf einem Feld der gleichen Farbe stehen. Schließlich sei $d > 0$ eine gegebene positive reelle Zahl.

Angenommen, es ist möglich, die Spielsteine so zu permutieren, dass jeder Spielstein höchstens im Abstand d bewegt wird und außerdem jeder Azur-Spielstein dorthin bewegt wird, wo vorher ein Bordeaux-Spielstein stand, jeder Bordeaux-Spielstein dorthin, wo vorher ein Citrin-Spielstein stand und jeder Citrin-Spielstein dorthin, wo vorher ein Azur-Spielstein stand. Zeige, dass es dann auch eine Permutation gibt, sodass jeder Spielstein höchstens im Abstand $d + 2$ bewegt wird und sodass jeder Spielstein danach auf einem Feld gleicher Farbe steht.

(Der Abstand zwischen zwei Feldern ist hierbei definiert als der euklidische Abstand zwischen den Mittelpunkten der Felder.)

Tipps zu den Beispielaufgaben

Tipp zu Aufgabe 1. Verheirate die Schalen mit passenden Kugeln.

Tipp zu Aufgabe 2. Du musst zeigen, dass Norman n Erdbeeren auswählen kann, sodass in jeder Zeile und jeder Spalte genau eine dieser Erdbeeren liegt. Verheirate dazu die Zeilen des Kuchens mit den Spalten des Kuchens.

Tipps zu Aufgabe 3. Verheirate die Zahlen $N + i$ für $i = 1, 2, \dots, n$ mit ihren Primfaktoren.

Um zu beweisen, dass die Bedingung des Heiratssatzes erfüllt ist, lasst euch von Aufgabe 4 inspirieren.

Tipps zu Aufgabe 4. Es gibt genau acht Primzahlen ≤ 20 .

Angenommen, $P(n)$ besitzt nur Primfaktoren ≤ 20 . Betrachte die größte Primpotenz, die $n + d_i$ teilt. Benutze dann das Schubfachprinzip.

Tipps zu Aufgabe 5. Verheirate Felder mit gleichfarbigen Spielsteinen.

Um die Bedingung des Heiratssatzes zum Beispiel für die Farbe Azur zu überprüfen, benutze, dass „durchschnittlich ein Drittel“ aller Felder Azur sind.

8 Multiplikative Ordnungen und Primitivwurzeln

In diesem Kapitel werden wir uns mit der Multiplikation auf den ganzen Zahlen modulo einer Zahl m befassen. Von zentraler Wichtigkeit ist hierbei die folgende Definition:

Definition. Sei a eine ganze Zahl, die teilerfremd zu m ist. Die *multiplikative Ordnung von a modulo m* , geschrieben $\text{ord}_m(a)$, ist die kleinste positive ganze Zahl mit der Eigenschaft

$$a^{\text{ord}_m(a)} \equiv 1 \pmod{m}.$$

Aus dem Satz von Euler-Fermat (siehe das Kapitel *Teiler und Teilerfremdheit* im Heft für die Klasse 9) folgt sofort, dass $\text{ord}_m(a) \leq \varphi(m)$. Tatsächlich können wir sogar noch mehr sagen:

Lemma. Sei a teilerfremd zu m . Für eine ganze Zahl n gilt genau dann $a^n \equiv 1 \pmod{m}$, wenn $\text{ord}_m(a)$ ein Teiler von n ist. Insbesondere ist $\text{ord}_m(a)$ stets ein Teiler von $\varphi(m)$.

Beachte, dass in diesem Lemma n auch negativ sein darf. Weil a zu m teilerfremd ist, besitzt a nämlich ein *multiplikatives Inverses modulo m* , es gibt also ein b mit $ab \equiv 1 \pmod{m}$ (zum Beispiel können wir $b = a^{\text{ord}_m(a)-1}$ wählen). Division durch a modulo m können wir dann als Multiplikation mit b interpretieren. Mehr dazu findet ihr im Kapitel *Teiler und Teilerfremdheit* im Heft für Klasse 9.

Beweis. Wenn n durch $\text{ord}_m(a)$ teilbar ist, können wir $n = \text{ord}_m(a)k$ schreiben. Dann folgt sofort $a^n \equiv (a^{\text{ord}_m(a)})^k \equiv 1^k \equiv 1 \pmod{m}$.

Umgekehrt bemerken wir, dass ganz allgemein aus $a^r \equiv 1 \pmod{m}$ und $a^s \equiv 1 \pmod{m}$ auch $a^{\text{ggT}(r,s)} \equiv 1 \pmod{m}$ folgt. Denn nach dem Lemma von Bezout gibt es ganze Zahlen u und v mit $ru + sv = \text{ggT}(r,s)$ und es folgt, wie gewünscht, $a^{\text{ggT}(r,s)} \equiv (a^r)^u \cdot (a^s)^v \equiv 1^u \cdot 1^v \equiv 1 \pmod{m}$. Wenn nun $a^n \equiv 1 \pmod{m}$ ist, dann muss n durch $\text{ord}_m(a)$ sein, denn ansonsten hätten wir $\text{ggT}(n, \text{ord}_m(a)) < \text{ord}_m(a)$, was die Minimalität von $\text{ord}_m(a)$ verletzen würde. \square

Primitivwurzeln

Das obige Lemma führt zu folgender naheliegender Frage: *Ist es möglich, dass ein a existiert, sodass $\text{ord}_m(a) = \varphi(m)$ gilt?*

Definition. Wenn ein solches a existiert, dann nennen wir es eine *Primitivwurzel modulo m* .

Es ist klar, dass die Existenz einer Primitivwurzel enorme Folgen für die Struktur der Multiplikation modulo m hätte. Wenn g eine Primitivwurzel modulo m ist, dann durchlaufen die Potenzen $g^0, g^1, g^2, \dots, g^{\varphi(m)-1}$ alle zu m teilerfremden Restklassen modulo m . Denn ihre Restklassen sind allesamt teilerfremd zu m und außerdem paarweise verschieden: Aus $g^i \equiv g^j \pmod{m}$ folgt $g^{i-j} \equiv 1 \pmod{m}$, weil wir durch die zu m teilerfremde Restklasse g dividieren dürfen. Nach dem Lemma ist also $i - j$ durch $\varphi(m) = \text{ord}_m(a)$ teilbar und wegen $0 \leq i, j < \varphi(m)$ kommt nur $i = j$ in Frage. Weil es insgesamt nur $\varphi(m)$ zu m teilerfremde Restklassen modulo m gibt, müssen die Potenzen $g^0, g^1, g^2, \dots, g^{\varphi(m)-1}$ sie alle durchlaufen, wie behauptet.

Im Spezialfall, dass $m = p$ eine Primzahl ist, sind alle Restklassen außer 0 zu p teilerfremd und wir würden erhalten, dass die Potenzen $g^0, g^1, g^2, \dots, g^{p-1}$ einer Primitivwurzel alle Restklassen $1, 2, \dots, p-1$ durchlaufen (wenn auch nicht notwendigerweise in dieser Reihenfolge).

Wir sehen also, dass es sehr praktisch ist, wenn eine Primitivwurzel existiert. Der folgende Satz verrät uns, wann das der Fall ist.

Satz von der Primitivwurzel. Eine Primitivwurzel modulo m existiert genau in den folgenden drei Fällen:

- (a) $m = 2$ oder $m = 4$.
- (b) $m = p^r$, wobei $p \geq 3$ eine ungerade Primzahl ist.
- (c) $m = 2p^r$, wobei $p \geq 3$ eine ungerade Primzahl ist.

Beweis. Wir überlegen uns zunächst, dass die Bedingung notwendig ist. Der Fall $m = 8$ lässt sich unmittelbar überprüfen.¹¹ Es folgt sofort, dass auch modulo 2^r für $r \geq 4$ keine Primitivwurzel existieren kann. Denn wäre g so eine Primitivwurzel, dann würden die Potenzen von g alle zu 2^r teilerfremden Restklassen modulo 2^r , also auch alle zu 8 teilerfremden Restklassen modulo 8, sodass g auch eine Primitivwurzel modulo 8 wäre.

Wenn nun m nicht von der Form $m = 2^r$, $m = p^r$ oder $m = 2p^r$ für eine ungerade Primzahl p ist, dann finden wir immer eine Zerlegung $m = uv$ in zwei teilerfremde Faktoren $u, v \geq 3$. Nach dem Chinesischen Restsatz gilt die Bedingung $a^n \equiv 1 \pmod{uv}$ genau dann, wenn sowohl die Bedingung $a^n \equiv 1 \pmod{u}$ als auch die Bedingung $a^n \equiv 1 \pmod{v}$ gilt. Hieraus folgt sofort, dass $\text{ord}_m(a)$ das kleinste gemeinsame Vielfache von $\text{ord}_u(a)$ und $\text{ord}_v(a)$ ist. Weil sich die Eulersche φ -Funktion für teilerfremde Faktoren multiplikativ verhält, gilt $\varphi(m) = \varphi(u)\varphi(v)$. Für $u, v \geq 3$ sind aber $\varphi(u)$ und $\varphi(v)$ beide durch 2 teilbar (das folgt zum Beispiel aus der expliziten Formel für φ ; siehe das Kapitel *Teiler und Teilerfremdheit* im Heft für Klasse 9). Also ist $\varphi(u)\varphi(v)$ strikt größer als das kleinste gemeinsame Vielfache von $\varphi(u)$ und $\varphi(v)$. Damit kann es modulo $m = uv$ keine Primitivwurzel geben.

Es bleibt zu zeigen, dass in den Fällen (b) und (c) stets eine Primitivwurzel existiert.

Schritt 1: Wir zeigen den Fall $m = p$. Das ist der schwierigste Fall und wir benötigen zwei Lemmata, die auch allgemein gut zu wissen sind.

Lemma 1. Sei $P(X)$ ein Polynom vom Grad n mit ganzzahligen Koeffizienten, sodass nicht alle Koeffizienten durch p teilbar sind. Dann hat $P(X)$ höchstens n Nullstellen modulo p .

Beweis. Wir benutzen Induktion nach n . Der Fall $n = 0$ ist klar: In diesem Fall ist $P(X)$ ein konstantes Polynom und diese Konstante kann nach Annahme nicht durch p teilbar sein. Also hat $P(X)$ keine Nullstellen modulo p .

Für den Induktionsschritt nehmen wir an, dass $n \geq 1$ gilt und die Aussage für Polynome vom Grad $\leq n - 1$ bereits bewiesen ist. Sei x_0 eine Nullstelle von $P(X)$ modulo p . Via Polynomdivision dividieren wir $P(X)$ durch $X - x_0$ modulo p . Beachte, dass Polynomdivision auch modulo p möglich ist. Denn um Polynomdivision wie üblich durchführen zu können, müssen wir nur durch den Leitkoeffizienten des Divisors teilen können. Der Leitkoeffizient von $X - x_0$ ist aber 1 und durch 1 können wir immer teilen.

Durch Polynomdivision mit Rest finden wir also Polynome $P_1(X)$ und $R_1(X)$ mit

$$P(X) \equiv (X - x_0)P_1(X) + R_1(X) \pmod{p}.$$

Ferner muss der Rest $R_1(X)$ kleineren Grad als $X - x_0$ haben (sonst könnten wir weiter polynomdividieren). Also muss $R_1(X) \equiv r \pmod{p}$ eine Konstante sein. Aus $P(x_0) \equiv 0 \pmod{p}$ folgt nun aber

$$0 \equiv P(x_0) \equiv (x_0 - x_0)P_1(x_0) + r \equiv r \pmod{p}.$$

Also ist $P(X) \equiv (X - x_0)P_1(X) \pmod{p}$.

Bis hierhin haben wir nicht gebraucht, dass n eine Primzahl ist, aber jetzt brauchen wir es: Wenn $x \not\equiv x_0 \pmod{p}$, dann ist $x - x_0$ eine teilerfremde Restklasse modulo p und wir können

¹¹Dass für $m = 8$ keine Primitivwurzel existiert, sorgt unter anderem dafür, dass Quadratzahlen modulo 8 nur die Reste 0, 1 und 4 lassen. Dieser Fakt hilft uns in vielen Olympiade-Aufgaben. Es ist also gar nicht so schlimm, dass es keine Primitivwurzel modulo 8 gibt.

durch $x - x_0$ teilen. Folglich kann $P(x) \equiv 0 \pmod{p}$ nur gelten, wenn schon $P_1(x) \equiv 0 \pmod{p}$ gilt. Alle von x_0 verschiedene Nullstellen von $P(X)$ sind also auch Nullstellen von $P_1(X)$. Es kann nicht sein, dass alle Koeffizienten von P_1 durch p teilbar sind, denn dann wäre selbiges auch für $P(X) = (X - x_1)P_1(X)$ erfüllt. Also können wir die Induktionsvoraussetzung auf $P_1(X)$ anwenden und finden heraus, dass $P_1(X)$ höchstens $n - 1$ Nullstellen hat. Zusammen mit x_0 kann $P(X)$ also höchstens n Nullstellen haben, wie gewünscht. \square

Lemma 2. Für alle positiven ganzen Zahlen n gilt

$$n = \sum_{d|n} \varphi(d),$$

wobei die Summe einmal durch alle positiven Teiler von n läuft.

Beweis. Für jeden Teiler $d | n$ gibt es genau $\varphi(n/d)$ positive ganze Zahlen $1 \leq k \leq n$ mit $\text{ggT}(k, n) = d$. Denn damit k durch d teilbar ist, muss $k = id$ für ein $1 \leq i \leq n/d$ gelten und damit k und n keinen größeren gemeinsamen Teiler haben, muss i zu n/d teilerfremd sein. Die Summe $\sum_{d|n} \varphi(n/d)$ zählt folglich jede Zahl $1 \leq k \leq n$ genau einmal und somit gilt $n = \sum_{d|n} \varphi(n/d)$. Wenn d einmal durch alle positiven Teiler von n läuft, dann läuft auch n/d einmal durch alle positiven Teiler von n . Also gilt $\sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d)$ und die Behauptung folgt. \square

Wenden wir uns nun wieder dem Problem zu, die Existenz einer Primitivwurzel modulo p nachzuweisen. Wir zeigen per Induktion, dass es für jeden Teiler $d | p - 1$ genau $\varphi(d)$ Restklassen von Ordnung d modulo p gibt. Im Falle $d = p - 1$ erhalten wir dann, dass es genau $\varphi(p - 1)$ Primitivwurzeln modulo p gibt. Insbesondere existiert mindestens eine.

Der Induktionsanfang $d = 1$ ist trivial, denn nur die Restklasse 1 hat Ordnung 1. Für den Induktionsschritt nehmen wir an, dass die Behauptung für alle echten Teiler $e | d$ bereits bewiesen ist. Es gilt

$$X^{p-1} - 1 = (X^d - 1) \left(1 + X^d + (X^d)^2 + \dots + (X^d)^{(p-1)/d-1} \right).$$

Nach Lemma 1 hat der erste Faktor $X^d - 1$ höchstens d Nullstellen und der zweite Faktor höchstens $(p - 1) - d$ Nullstellen. Nach dem kleinen Satz von Fermat hat das Polynom $X^{p-1} - 1$ jedoch genau $p - 1$ Nullstellen modulo p , nämlich $1, 2, \dots, p - 1$. Somit muss auch $X^d - 1$ genau d Nullstellen besitzen. Für jeden Teiler $e | d$ sind die Restklassen von Ordnung e allesamt Nullstellen von $X^d - 1$. Nach Induktionsannahme gibt es für jeden echten Teiler $e | d$ genau $\varphi(e)$ Restklassen von Ordnung e . Damit haben wir $\sum_{e|d, e \neq d} \varphi(e)$ Nullstellen von $X^d - 1$ identifiziert. Nach Lemma 2 bleiben genau $\varphi(d)$ Nullstellen übrig. Jede solche Nullstelle x erfüllt einerseits $x^d \equiv 1 \pmod{p}$, kann aber andererseits nicht Ordnung e für irgendeinen echten Teiler $e | d$ haben. Also muss $\text{ord}_p(x) = d$ gelten. Damit haben wir gezeigt, dass genau $\varphi(d)$ Restklassen mit dieser Eigenschaft existieren. Das beendet den Induktionsschritt, die Induktion sowie den Beweis im Fall $m = p$.

Schritt 2: Wir zeigen den Fall $m = p^2$. Sei g eine Primitivwurzel modulo p . Wir wollen die Ordnung von g modulo p^2 untersuchen. Es ist klar, dass $\text{ord}_{p^2}(g)$ durch $\text{ord}_p(g) = p - 1$ teilbar ist, denn aus $g^{\text{ord}_{p^2}(g)} \equiv 1 \pmod{p^2}$ folgt auch $g^{\text{ord}_{p^2}(g)} \equiv 1 \pmod{p}$. Andererseits muss $\text{ord}_{p^2}(g)$ ein Teiler von $\varphi(p^2) = (p - 1)p$ sein. Also kommen nur die Möglichkeiten $\text{ord}_{p^2}(g) = p - 1$ und $\text{ord}_{p^2}(g) = (p - 1)p$ in Frage. Im zweiten Fall ist g eine Primitivwurzel modulo p^2 und wir sind fertig. Im ersten Fall behaupten wir, dass $g + p$ eine Primitivwurzel modulo p^2 ist. Wegen $g + p \equiv g \pmod{p}$ muss $g + p$ auf jeden Fall eine Primitivwurzel modulo p sein. Nach dem gleichen Argument wie oben müssen wir also nur den Fall $\text{ord}_{p^2}(g + p) = p - 1$ ausschließen. Dazu rechnen wir

$$(g + p)^{p-1} \equiv \sum_{k=0}^{p-1} \binom{p-1}{k} p^k g^{p-1-k} \equiv g^{p-1} + (p-1)pg^{p-2} \pmod{p^2}.$$

Hier haben wir benutzt, dass für $k \geq 2$ alle Terme in der Summe durch p^2 teilbar sind. Nach Annahme ist $g^{p-1} \equiv 1 \pmod{p^2}$, aber $(p-1)pg^{p-2}$ kann nicht durch p^2 teilbar sein. Folglich ist $(g+p)^{p-1} \not\equiv 1 \pmod{p^2}$, wie gewünscht.

Schritt 3: Wir zeigen den allgemeinen Fall $m = p^r$. Sei g eine Primitivwurzel modulo p^2 . Wir zeigen nun per Induktion nach r , dass g auch eine Primitivwurzel modulo p^r für alle $r \geq 2$ ist. Der Induktionsanfang $r = 2$ ist unsere Annahme an g . Nun sei $r \geq 3$ und wir nehmen an, dass wir bereits bewiesen haben, dass g eine Primitivwurzel modulo p^{r-1} ist. Analog zum Fall $m = p^2$ sehen wir, dass $\text{ord}_{p^r}(g)$ durch $\text{ord}_{p^{r-1}}(g) = \varphi(p^{r-1}) = (p-1)p^{r-2}$ teilbar sein muss. Andererseits ist $\text{ord}_{p^r}(g)$ ein Teiler von $\varphi(p^r) = (p-1)p^{r-1}$. Es kommen also nur die Möglichkeiten $\text{ord}_{p^r}(g) = (p-1)p^{r-2}$ oder $\text{ord}_{p^r}(g) = (p-1)p^{r-1}$ in Frage. Im zweiten Fall sind wir fertig, also müssen wir nur den ersten Fall ausschließen. Nach dem Satz von Euler-Fermat gilt $g^{(p-1)p^{r-3}} \equiv 1 \pmod{p^{r-2}}$, jedoch ist $g^{(p-1)p^{r-3}} \not\equiv 1 \pmod{p^{r-1}}$, denn g ist Primitivwurzel modulo p^{r-1} . Somit können wir $g^{(p-1)p^{r-3}} = 1 + ap^{r-2}$ schreiben, wobei a nicht durch p teilbar ist. Wir rechnen nun

$$g^{(p-1)p^{r-2}} \equiv \left(g^{(p-1)p^{r-3}}\right)^p \equiv \left(1 + ap^{r-2}\right)^p \equiv \sum_{k=0}^p \binom{p}{k} a^k p^{k(r-2)} \equiv 1 + \binom{p}{1} ap^{r-2} \pmod{p^r}.$$

Hier haben wir folgendes benutzt: Für $k \geq 3$ sind alle Terme in der Summe durch p^r teilbar, denn $k(r-2) \geq r$ ist äquivalent zu $(k-1)(r-2) \geq 2$, was für $r, k \geq 3$ erfüllt ist. Für $k = 2$ ist der Binomialkoeffizient $\binom{p}{2} = \frac{(p-1)p}{2}$ durch p teilbar, denn p ist eine ungerade Primzahl.¹² Folglich ist $\binom{p}{2} a^2 p^{2(r-2)}$ mindestens durch p^{2r-3} teilbar, also auch durch p^r , denn $r \geq 3$. Wir bemerken nun, dass $1 + \binom{p}{1} ap^{r-2} \equiv 1 + ap^{r-1} \not\equiv 1 \pmod{p^r}$, denn a ist nach Annahme nicht durch p teilbar.

Schritt 4: Wir zeigen den Fall $m = 2p^r$. Dieser Fall ist einfach: Weil p eine ungerade Primzahl ist und g eine Primitivwurzel modulo p^r , muss genau eine der beiden Zahlen g oder $g + p^r$ ungerade sein. Genau eine dieser beiden Zahlen ist also teilerfremd zu $2p^r$. Ihre Ordnung modulo $2p^r$ kann nicht kleiner als ihre Ordnung modulo p^r sein. Andererseits ist $\varphi(2p^r) = \varphi(2)\varphi(p^r) = \varphi(p^r)$. Die betrachtete Zahl ist also automatisch auch eine Primitivwurzel modulo $2p^r$.

Das beendet den Beweis des Satzes von der Primitivwurzel. □

Ordnungen in Olympiade-Aufgaben

Der Satz von der Primitivwurzel ist gelegentlich in Olympiade-Aufgaben hilfreich. Die Überlegungen, die in den Beweis geflossen sind – insbesondere die beiden Lemmata in Schritt 1 sowie die Betrachtungen in Schritt 2 und 3 – sind sogar richtig nützlich und kommen häufig unabhängig von Primitivwurzeln zur Anwendung. Das Allernützlichste in diesem Kapitel ist aber das Prinzip der Ordnung selbst: Erstaunlich viele Zahlentheorie-Aufgaben lassen sich lösen, indem ihr euch die richtigen Ordnungen anschaut!

Ein häufiger Trick bei solchen Aufgaben ist, dass ihr euch den kleinsten Primfaktor eines der auftretenden Exponenten anschaut. Denn wenn p der kleinste Primfaktor von n ist, dann sind $p-1$ und n teilerfremd – also kann eine Ordnung, die n und $p-1$ teilt, nur gleich 1 sein.

Ihr sollt nun einige solche Aufgaben selbstständig lösen, um euch mit der Methode vertraut zu machen. Am Ende dieses Kapitels findet ihr Tipps zu den Aufgaben und am Ende dieses Heftes findet ihr Lösungen.

¹²Das ist das erste und einzige Mal, dass wir diese Voraussetzung benutzen. Im Fall $p = 2$, $r = 3$ geht der Beweis genau an dieser Stelle schief.

Aufgabe 1. Gegeben seien positive ganze Zahlen a und n , wobei $a \geq 2$. Zeige, dass n ein Teiler von $\varphi(a^n - 1)$ ist.

Aufgabe 2.

(a) Sei $n \geq 2$ eine positive ganze Zahl, sei p eine Primzahl und sei q ein Primteiler von $\frac{n^p-1}{n-1}$. Zeige, dass stets $q = p$ oder $q \equiv 1 \pmod{p}$ gilt.

(b) Zeige, dass es unendlich viele Primzahlen q mit $q \equiv 1 \pmod{p}$ gibt.

Aufgabe 2(b) ist offensichtlich ein Spezialfall des berühmten *Primzahlsatzes von Dirichlet*:

Primzahlsatz von Dirichlet. Gegeben seien teilerfremde positive ganze Zahlen a und m . Dann gibt es unendlich viele Primzahlen q mit $q \equiv a \pmod{m}$.

Der Beweis dieses Satzes benutzt komplexe Analysis und geht damit weit über unsere Methoden hinaus. Demzufolge wird es nicht gern gesehen, wenn ihr den Primzahlsatz von Dirichlet in einer Olympiade verwendet (aber wenn ihr so eine Lösung findet, schreibt ihr sie natürlich trotzdem auf). Es ist also nützlich, einige Spezialfälle zu kennen, die sich auch mit elementaren Methoden zeigen lassen. Aufgabe 2(b) ist einer davon; in Kapitel 9: *Quadratische Reste* werdet ihr einen weiteren Spezialfall sehen.

Aufgabe 3*. Finde alle Paare (n, p) , wobei p eine Primzahl ist und $n \leq 2p$ eine positive ganze Zahl, sodass n^{p-1} ein Teiler von $(p-1)^n + 1$ ist.

Aufgabe 4*. Finde alle Paare (p, q) von Primzahlen, sodass pq ein Teiler von $5^p + 5^q$ ist.

Aufgabe 5.** Beweise, dass es unendlich viele Paare (p, q) von Primzahlen mit $p \neq q$ gibt, sodass p ein Teiler von $2^{q-1} - 1$ und q ein Teiler von $2^{p-1} - 1$ ist.

Tipps zu den Beispielaufgaben

Typ zu Aufgabe 1. Schreibe n als die Ordnung einer geeigneten Zahl modulo $a^n - 1$.

Tipps zu Aufgabe 2. Für (a), betrachte die Ordnung von n modulo q . Was kannst du über diese Ordnung aussagen?

Für (b), benutze (a) und argumentiere analog zu dem üblichen Beweis, dass es unendlich viele Primzahlen gibt.

Tipps zu Aufgabe 3. Betrachte den kleinsten Primfaktor q von n sowie die Ordnung von $p-1$ modulo q .

Um den Fall $n = p$ zu lösen, betrachte alles modulo p^3 .

Tipps zu Aufgabe 4. Benutze den kleinen Satz von Fermat und betrachte die Ordnung von 5 modulo p und modulo q .

Um den Fall $p, q \neq 5$ zum Widerspruch zu führen, untersuche genau, wie oft $p-1$, $q-1$ sowie $\text{ord}_p(5)$ und $\text{ord}_q(5)$ durch 2 teilbar sein müssen.

Typ zu Aufgabe 5. Betrachte Primfaktoren von $2^{2^r} - 1$, wobei r eine Primzahl ist.

9 Quadratische Reste

In diesem Kapitel führen wir die Überlegungen aus dem vorherigen Kapitel fort und untersuchen, wann eine Restklasse modulo einer Primzahl das Quadrat einer anderen Restklasse ist.

Allgemeine Theorie

Definition. Sei p eine Primzahl. Eine Restklasse a modulo p heißt *quadratischer Rest modulo p* , wenn es eine Restklasse b mit $a \equiv b^2 \pmod{p}$ gibt. Ansonsten wird a *quadratischer Nichtrest modulo p* genannt.

Lemma. Für jede ungerade Primzahl p gibt es genau $1 + \frac{p-1}{2}$ quadratische Reste.

Beweis. Offensichtlich ist 0 ein quadratischer Rest. Wir wissen aus dem vorherigen Kapitel, dass eine Primitivwurzel g modulo p existiert, sodass die Potenzen g^0, g^1, \dots, g^{p-1} genau die Restklassen $1, 2, \dots, p-1$ durchlaufen (nicht notwendigerweise in dieser Reihenfolge). Die quadratischen Reste außer 0 sind dann genau die geraden Potenzen von g , also g^0, g^2, \dots, g^{p-1} . Also gibt es außer 0 noch $\frac{p-1}{2}$ weitere quadratische Reste. \square

Um quadratische Reste von quadratischen Nichtresten zu unterscheiden, führen wir die folgende Notation ein:

Definition. Sei $p \geq 3$ eine ungerade Primzahl und sei a eine Restklasse modulo p . Das *Legendre-Symbol von a modulo p* ist definiert als

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{falls } a \equiv 0 \pmod{p} \\ 1 & \text{falls } a \text{ quadratischer Rest modulo } p \text{ ist} \\ -1 & \text{falls } a \text{ quadratischer Nichtrest modulo } p \text{ ist} \end{cases}.$$

Lasst euch von der etwas gewöhnungsbedürftigen Notation nicht verwirren: Das Legendre-Symbol $\left(\frac{a}{p}\right)$ hat natürlich nichts mit dem Bruch $\frac{a}{p}$ zu tun.

Das Legendre-Symbol hat einige nützliche alternative Beschreibungen. Die beiden einfachsten solchen Beschreibungen sind das *Euler-Kriterium* und das *Gauß-Lemma*.

Euler-Kriterium. Sei $p \geq 3$ eine ungerade Primzahl und sei a eine Restklasse modulo p . Dann gilt stets

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Beweis. Für $a \equiv 0 \pmod{p}$ ist das Euler-Kriterium offensichtlich. Sei nun a teilerfremd zu p . Nach dem kleinen Satz von Fermat ist $(a^{(p-1)/2})^2 \equiv a^{p-1} \equiv 1 \pmod{p}$. Folglich muss $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$ gelten, denn das Polynom $X^2 - 1$ hat modulo p genau die Nullstellen ± 1 (weil es sich zu $X^2 - 1 = (X-1)(X+1)$ faktorisieren lässt). Für müssen also nur zeigen, dass der Fall $a^{(p-1)/2} \equiv 1 \pmod{p}$ genau dann eintritt, wenn a ein quadratischer Rest ist. Dafür benutzen wir wieder, dass modulo p eine Primitivwurzel g existiert. Schreibe also $a \equiv g^k \pmod{p}$ mit $0 \leq k \leq p-1$. Wir wissen, dass a genau dann ein quadratischer Rest ist, wenn k gerade ist. Andererseits ist $k \frac{p-1}{2}$ genau dann durch $p-1$ teilbar, wenn k gerade ist. Somit gilt auch $g^{k(p-1)/2} \equiv 1 \pmod{p}$ genau dann, wenn k gerade ist. Das ist genau, was wir zeigen wollten. \square

Gauß-Lemma. Sei $p \geq 3$ eine ungerade Primzahl und a eine Restklasse modulo p , die zu p teilerfremd ist. Sei ferner μ die Anzahl aller Restklassen $r \in \{1, 2, \dots, \frac{p-1}{2}\}$, sodass der Rest von ar modulo p in $\{\frac{p-1}{2} + 1, \frac{p-1}{2} + 2, \dots, p-1\}$ liegt. Dann gilt

$$\left(\frac{a}{p}\right) = (-1)^\mu.$$

Beweis. Der Beweis ist sehr ähnlich zum Beweis des Satzes von Euler-Fermat. Wir beobachten zuerst, dass für $r, s \in \{1, 2, \dots, \frac{p-1}{2}\}$ mit $r \neq s$ stets $ar \not\equiv as \pmod{p}$ und $ar \not\equiv -as \pmod{p}$ gilt. Denn Ersteres würde $r \equiv s \pmod{p}$ implizieren und Zweiteres würde $r \equiv -s \pmod{p}$ implizieren, beides ist unmöglich. Es folgt: Wenn r die Menge $\{1, 2, \dots, \frac{p-1}{2}\}$ durchläuft, dann bilden die Reste von ar modulo p bis aufs Vorzeichen eine Permutation von $\{1, 2, \dots, \frac{p-1}{2}\}$. Aus der Definition von μ folgt ferner, dass besagtes Vorzeichen genau μ mal negativ ist. Folglich ist

$$a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \equiv \prod_{r=1}^{\frac{p-1}{2}} ar \equiv (-1)^\mu \prod_{r=1}^{\frac{p-1}{2}} r \equiv (-1)^\mu \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Weil $\left(\frac{p-1}{2}\right)!$ teilerfremd zu p ist, dürfen wir modulo p dadurch dividieren. Damit erhalten wir $a^{(p-1)/2} \equiv (-1)^\mu \pmod{p}$. Indem wir nun das Euler-Kriterium anwenden, sind wir fertig. \square

Der wichtigste Satz über das Legendre-Symbol ist das *Quadratische Reziprozitätsgesetz*, das von zwei Ergänzungssätzen begleitet wird.

Quadratisches Reziprozitätsgesetz (QRG). Wenn $p, q \geq 3$ zwei verschiedene ungerade Primzahlen sind, dann gilt stets

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right).$$

Erster Ergänzungssatz zum QRG. Für jede ungerade Primzahl $p \geq 3$ gilt

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{falls } p \equiv 1 \pmod{4} \\ -1 & \text{falls } p \equiv 3 \pmod{4} \end{cases}$$

Beweis. Das folgt sofort aus dem Euler-Kriterium. \square

Zweiter Ergänzungssatz zum QRG. Für jede ungerade Primzahl $p \geq 3$ gilt

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{falls } p \equiv 1, 7 \pmod{8} \\ -1 & \text{falls } p \equiv 3, 5 \pmod{8} \end{cases}$$

Beweis. Übungsaufgabe. (Tipp: Benutze das Gauß-Lemma.) \square

Bevor wir das QRG beweisen, werden wir erklären, wie sich dadurch Legendre-Symbole sehr einfach berechnen lassen. Insbesondere lässt sich sehr einfach entscheiden, ob eine gegebene Restklasse ein quadratischer Rest oder ein quadratischer Nichtrest ist. Der Ausgangspunkt dieser Methode ist die Beobachtung, dass das Legendre-Symbol *multiplikativ* ist: Es gilt

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$

Diese Beobachtung folgt sofort aus dem Euler-Kriterium, denn $(ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \pmod{p}$. Um das Legendre-Symbol $\left(\frac{a}{p}\right)$ zu berechnen, genügt es also, a in Primfaktoren zu zerlegen und für jeden Primfaktor q von a das Legendre-Symbol $\left(\frac{q}{p}\right)$ auszurechnen. Wenn $q > p$, dann können wir q durch seinen Rest r modulo p ersetzen und stattdessen $\left(\frac{r}{p}\right)$ berechnen. Dazu zerlegen wir r wieder in Primfaktoren und so weiter. Wenn $q = p$, dann ist offensichtlich $\left(\frac{q}{p}\right) = 0$. Im Fall $q < p$ wenden wir schließlich das QRG an, was die Berechnung von $\left(\frac{q}{p}\right)$ auf die Berechnung von $\left(\frac{p}{q}\right)$ reduziert. Dann können wir p durch seinen Rest s modulo q ersetzen, s in Primfaktoren zerlegen und so weiter. Nach endlich vielen Schritten müssen wir in einer Situation angelangt sein, in der sich einer der beiden Ergänzungssätze oder eine der beiden trivialen Gleichungen $\left(\frac{0}{p}\right) = 0$ und $\left(\frac{1}{p}\right) = 1$ anwenden lässt.

Hier seht ihr eine Beispielrechnung:

$$\begin{aligned} \left(\frac{42}{1777}\right) &= \left(\frac{2}{1777}\right) \left(\frac{3}{1777}\right) \left(\frac{7}{1777}\right) = 1 \cdot (-1)^{\frac{3-1}{2} \cdot \frac{1777-1}{2}} \left(\frac{1777}{3}\right) \cdot (-1)^{\frac{7-1}{2} \cdot \frac{1777-1}{2}} \left(\frac{1777}{7}\right) \\ &= \left(\frac{1}{3}\right) \left(\frac{6}{7}\right) = 1 \cdot \left(\frac{2}{7}\right) \left(\frac{3}{7}\right) = 1 \cdot (-1)^{\frac{3-1}{2} \cdot \frac{7-1}{2}} \left(\frac{7}{3}\right) = (-1) \cdot \left(\frac{1}{3}\right) = (-1) \cdot 1 \\ &= -1. \end{aligned}$$

Es gibt eine Menge unterschiedlicher Beweise für das QRG. Viele dieser Beweise benutzen Methoden der Algebraischen Zahlentheorie, die ihr erst im Studium kennenlernen werdet. Dafür decken sie die tieferen Gründe auf, die hinter dem QRG stehen. Der Beweis, den wir präsentieren werden, offenbart zwar keine tieferen Zusammenhänge, ist aber deshalb nicht weniger schön. Er geht auf Gotthold Eisenstein (1823–1852) zurück.

Beweis des QRG. Wir benutzen das Gauß-Lemma. Sei μ die Anzahl aller $x \in \{1, 2, \dots, \frac{p-1}{2}\}$, sodass der Rest von qx modulo p in $\{\frac{p-1}{2} + 1, \frac{p-1}{2} + 2, \dots, p-1\}$ liegt und sei v die Anzahl aller Restklassen $y \in \{1, 2, \dots, \frac{q-1}{2}\}$, sodass der Rest von py modulo q in $\{\frac{q-1}{2} + 1, \frac{q-1}{2} + 2, \dots, q-1\}$ liegt. Nach dem Gauß-Lemma gilt dann $\left(\frac{q}{p}\right) = (-1)^\mu$ und $\left(\frac{p}{q}\right) = (-1)^v$. Um das QRG zu zeigen, müssen wir nur zeigen, dass $\mu + v$ die gleiche Parität wie $\frac{p-1}{2} \cdot \frac{q-1}{2}$ hat.

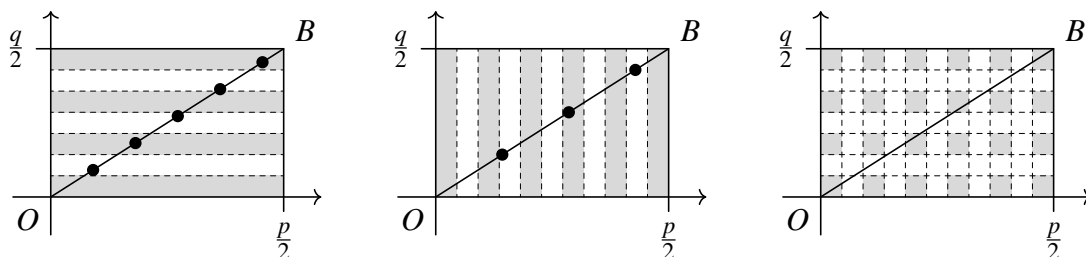
Dafür ist es praktischer, diejenigen Restklassen $x \in \{1, 2, \dots, \frac{p-1}{2}\}$ zu betrachten, sodass der Rest von qx modulo p ebenfalls in $\{1, 2, \dots, \frac{p-1}{2}\}$ liegt. Nach Definition von μ gibt es genau $\frac{p-1}{2} - \mu$ solche Restklassen x . Eine Restklasse x erfüllt diese Bedingung genau dann, wenn es eine ganze Zahl y gibt, sodass

$$py + 1 \leq qx \leq py + \frac{p-1}{2}.$$

Um diese Bedingung zu vereinfachen, fällt uns auf, dass $py = qx$ nicht eintreten kann, denn dafür müsste x durch p teilbar sein. Also ist $py + 1 \leq qx$ äquivalent zu $py \leq qx$. Ferner ist $qx \leq py + \frac{p-1}{2}$ äquivalent zu $qx \leq py + \frac{p}{2}$, weil $\frac{p}{2}$ ja gar keine ganze Zahl ist. Wir können die Bedingung also durch $py \leq qx \leq py + \frac{p}{2}$ ersetzen. Nach Division durch p erhalten wir

$$y \leq \frac{q}{p}x \leq y + \frac{1}{2}.$$

Wir wollen diese Bedingung geometrisch interpretieren. Betrachte das Rechteck $OABC$ mit den Eckpunkten $O = (0, 0)$, $A = (\frac{p}{2}, 0)$, $B = (\frac{p}{2}, \frac{q}{2})$ und $C = (0, \frac{q}{2})$. Für $y = 0, 1, 2, \dots, \frac{q-1}{2}$ betrachten wir den horizontalen Streifen aller Punkte (s, t) mit $y \leq t \leq y + \frac{1}{2}$. In der ersten Abbildung unten haben wir diese horizontalen Streifen grau eingefärbt. Dann zählt $\frac{p-1}{2} - \mu$ wieviele der Punkte $(x, \frac{q}{p}x)$ für $x = 1, 2, \dots, \frac{p-1}{2}$ in einem horizontalen grauen Streifen liegen.



Analog können wir für $x = 0, 1, 2, \dots, \frac{p-1}{2}$ den vertikalen Streifen aller Punkte (s, t) betrachten, für die $x \leq s \leq x + \frac{1}{2}$ gilt. In der zweiten Abbildung sind diese vertikalen Streifen grau eingefärbt.

Dann zählt $\frac{q-1}{2} - v$ wieviele der Punkte $(\frac{p}{q}y, y)$ für $y = 1, 2, \dots, \frac{q-1}{2}$ in einem vertikalen grauen Streifen liegen. Die Überschneidungen der horizontalen und vertikalen grauen Streifen sind kleine Quadrate, die wir in der dritten Abbildung grau eingefärbt haben.

Für jedes x liegt der Punkt $(x, \frac{q}{p}x)$ auf dem linken Rand eines vertikalen grauen Streifens. Also zählt $\frac{p-1}{2} - \mu$ auch, wie oft die Diagonale \overline{OB} den linken Rand eines kleinen grauen Quadrats trifft. Analog zählt $\frac{q-1}{2} - v$ auch, wie oft die Diagonale \overline{OB} den unteren Rand eines kleinen grauen Quadrates trifft (das kleine graue Quadrat mit Eckpunkt O wird in beiden Fällen nicht mitgezählt). Folglich zählt

$$\lambda := \frac{p-1}{2} - \mu + \frac{q-1}{2} - v + 1 = \frac{p+q}{2} - (\mu + v),$$

wieviele der kleinen grauen Quadrate die Diagonale \overline{OB} schneidet (das $+1$ am Ende sorgt dafür, dass diesmal das Quadrat mit Eckpunkt O mitgezählt wird). Da wir nur an der Parität von $\mu + v$ interessiert sind, müssen wir nur die Parität von λ bestimmen, also die Parität der Anzahl der Schnitte von \overline{OB} mit den kleinen grauen Quadraten.

Wenn wir das Rechteck $OABC$ um seinen Mittelpunkt um 180° drehen, wird \overline{OB} auf sich selbst und jedes kleine graue Quadrat auf ein kleines graues Quadrat abgebildet. Damit können wir die kleinen grauen Quadrate, die von \overline{OB} geschnitten werden, in Paare aufteilen – es sei denn, eines der kleinen grauen Quadrate wird bei der Drehung auf sich selbst abgebildet. Dieses Quadrat müsste dann genau in der Mitte von $OABC$ sitzen. Ein solches Quadrat existiert genau dann, wenn die Anzahl der kleinen grauen Quadrate, also $\frac{p+1}{2} \cdot \frac{q+1}{2}$, ungerade ist. Wir sehen also, dass λ die gleiche Parität wie $\frac{p+1}{2} \cdot \frac{q+1}{2}$ hat. Folglich hat $-(\mu + v) = \lambda - \frac{p+q}{2}$ die gleiche Parität wie $\frac{p+1}{2} \cdot \frac{q+1}{2} - \frac{p+q}{2} = \frac{p-1}{2} \cdot \frac{q-1}{2}$. Also hat auch $\mu + v$ die gleiche Parität wie $\frac{p-1}{2} \cdot \frac{q-1}{2}$ und wir sind fertig! \square

Beispielaufgaben

Die Theorie der quadratischen Reste lässt sich auf vielfältige Weise in Olympiade-Aufgaben anwenden. Eine Anwendung haben wir im letzten Kapitel schon gesehen: Wir können sehr leicht bestimmen, ob eine gegebene Restklasse ein quadratischer Rest ist. Aber es gibt noch viele weitere Tricks, die ihr euch in den folgenden Aufgaben selbst erarbeiten sollt.

Wie üblich findet ihr am Ende des Kapitels Tricks zu den Aufgaben und am Ende des Heftes könnt ihr die Lösungen nachlesen.

Aufgabe 1.

- (a) Zeige, dass es unendlich viele Primzahlen p mit $p \equiv 3 \pmod{4}$ gibt.
- (b) Zeige, dass es unendlich viele Primzahlen p mit $p \equiv 1 \pmod{4}$ gibt.

Aufgabe 2*. Seien a und b zwei positive ganze Zahlen mit der Eigenschaft, dass sowohl $15a + 16b$ als auch $16a - 15b$ Quadratzahlen sind. Finde den kleinstmöglichen positiven Wert, den das Minimum der beiden Quadratzahlen annehmen kann.

Aufgabe 3*. Sei a eine ganze Zahl. Zeige, dass die Zahlen $a^2 + 3$ und $a^2 + 5$ niemals Kubikzahlen sein können.

Aufgabe 3 benutzt einen Trick, der sehr gut zu wissen, aber nur sehr schwer zu finden ist. Benutzt also gerne die Tipps, dazu sind sie schließlich da.

Aufgabe 4.** Sei p eine Primzahl und r eine Restklasse modulo p , die $r^7 \equiv 1 \pmod{p}$ erfüllt. Zeige: Wenn $r + 1$ und $r^2 + 1$ quadratische Reste modulo p sind, dann ist auch $r^3 + 1$ ein quadratischer Rest modulo p .

Tipps zu den Beispielaufgaben

Tipps zu Aufgabe 1. Beide Teilaufgaben funktionieren ähnlich wie der übliche Beweis, dass unendlich viele Primzahlen existieren. Für (a) überlege dir, wie du erzwingen kannst, dass eine ganze Zahl einen Primfaktor $\equiv 3 \pmod{4}$ besitzt. Für (b) benutze den ersten Ergänzungssatz zum QRG.

Tipps zu Aufgabe 2. Löse das lineare Gleichungssystem $15a + 16b = m^2$, $16a - 15b = n^2$. Welche Bedingungen müssen m^2 und n^2 erfüllen, damit die Lösungen ganzzahlig sind?

Zeige, dass 15 kein quadratischer Rest modulo den Primfaktoren von $15^2 + 16^2$ ist.

Tipps zu Aufgabe 3. Um zu zeigen, dass $a^2 + 5 = b^3$ keine Lösungen hat, schreibe die Gleichung in der Form $a^2 + 4 = b^3 - 1$. Also muss -4 ein quadratischer Rest modulo jedem Primfaktor von $b^3 - 1$ sein. Folgere daraus einen Widerspruch.

Zu zeigen, dass $a^2 + 3 = b^3$ keine Lösung hat, geht mit einem ähnlichen Argument (dieses braucht allerdings ein paar Schritte mehr).

Tipps zu Aufgabe 4. Betrachte das Produkt $(r+1)(r^2+1)(r^3+1)$.

Wie lässt sich die Bedingung $r^7 \equiv 1 \pmod{p}$ mithilfe einer Primitivwurzel modulo p ausdrücken? Zeige, dass r ein quadratischer Rest modulo p sein muss.

Lösungen zu den Beispielaufgaben

Die Lösungen sind nicht immer so formuliert, wie ihr das in der Olympiade tun solltet. Zum Teil sind sie sehr knapp – zum Beispiel überspringen wir triviale Umformungsschritte oder lassen die Probe weg. In der Olympiade solltet ihr etwas ausführlicher sein und immer die Probe machen. Umgekehrt erklären wir gelegentlich (vor allem bei besonders schweren Aufgaben), wie wir auf die Lösung gekommen sind. In der Olympiade müsst ihr solche Überlegungen natürlich nicht aufschreiben, sondern könnt eure ausgefuchste Lösung einfach vom Himmel fallen lassen.

Soweit bekannt ist außerdem angegeben, aus welchem Wettbewerb die betreffende Aufgabe stammt, damit ihr (zum Beispiel in einschlägigen Foren) nach Alternativlösungen suchen könnt.

Lösungen zu Kapitel 2: Die Schuirhead-Ungleichung

Lösung zu Aufgabe 1 (IMO 1984). Diese Aufgabe haben wir schon im Heft für die Klasse 9 mit der Schiebemethode gelöst. Hier lösen wir sie noch einmal mit Schuirhead. Wegen $x + y + z = 1$ ist die Ungleichung äquivalent zu

$$0 \leq (x + y + z)(xy + yz + zx) - 2xyz \leq \frac{7}{27}(x + y + z)^3.$$

Diese Ungleichung ist invariant unter Skalierung der Variablen, also können wir die Nebenbedingung $x + y + z = 1$ ab jetzt ignorieren (dieser Trick nennt sich *Homogenisierung* und sollte fester Bestandteil eures Ungleichungs-Repertoires sein). Die linke Ungleichung wird nun zu $0 \leq x^2y + xy^2 + y^2z + yz^2 + z^2x + zx^2 + xyz$, was trivialerweise wahr ist. Durch Ausmultiplizieren und Vereinfachen wird die rechte Ungleichung zu

$$6(x^2y + xy^2 + y^2z + yz^2 + z^2x + zx^2) \leq 7(x^3 + y^3 + z^3) + 15xyz.$$

Aus der Schur-Ungleichung folgt $5(x^2y + xy^2 + y^2z + yz^2 + z^2x + zx^2) \leq 5(x^3 + y^3 + z^3) + 15xyz$ und aus Muirhead folgt $x^2y + xy^2 + y^2z + yz^2 + z^2x + zx^2 \leq 2(x^3 + y^3 + z^3)$. \square

Lösung zu Aufgabe 2. Wenn wir die Schur-Ungleichung $x^3 + y^3 + z^3 + 3xyz \geq x^2y + xy^2 + y^2z + yz^2 + z^2x + zx^2$ mit $x + y + z$ multiplizieren, erhalten wir nach Vereinfachung die Ungleichung

$$(x^4 + y^4 + z^4) + (x^2yz + y^2zx + z^2xy) \geq 2(x^2y^2 + y^2z^2 + z^2x^2).$$

Die Muirhead-Ungleichungen $T_{(4,0,0)}(x, y, z) \geq T_{(2,2,0)}(x, y, z)$ und $T_{(3,1,0)}(x, y, z) \geq T_{(2,2,0)}(x, y, z)$ liefern

$$2(x^4 + y^4 + z^4) + (x^3y + xy^3 + y^3z + yz^3 + z^3x + zx^3) \geq 2(x^2y^2 + y^2z^2 + z^2x^2).$$

Wenn wir diese beiden Ungleichungen addieren, erhalten wir genau die ausmultiplizierte Form der Behauptung. \square

Lösungen zu Kapitel 3: Die Ungleichungen von Jensen und Karamata

Lösung zu Aufgabe 1. Falls ein Index i mit $a_i = 0$ existiert, ist $\sqrt[n]{a_1 a_2 \cdots a_n} = 0$ und die AM-GM-Ungleichung ist trivial. Also dürfen wir annehmen, dass alle a_i positiv sind. Dann gibt es reelle Zahlen x_1, x_2, \dots, x_n mit $a_i = e^{x_i}$. Die Exponentialfunktion $f(x) = e^x$ ist konvex, denn es gilt $f''(x) = e^x > 0$. Aus der Jensenschen Ungleichung folgt also

$$\frac{e^{x_1} + e^{x_2} + \cdots + e^{x_n}}{n} \geq e^{(x_1 + x_2 + \cdots + x_n)/n} = \sqrt[n]{e^{x_1} e^{x_2} \cdots e^{x_n}}.$$

Indem wir $a_i = e^{x_i}$ einsetzen, erhalten wir genau die AM-GM-Ungleichung. Damit haben wir Teilaufgabe (a) gelöst.

Für (b) substituieren wir $y_i = a_i^q$, sodass $a_i^p = y_i^{p/q}$. Die Funktion $g(x) = x^{p/q}$ ist konvex, denn

$$g''(x) = \frac{p}{q} \left(\frac{p}{q} - 1 \right) x^{p/q-2} > 0$$

für alle $x > 0$ (hier benutzen wir $p > q$). Aus der Jensenschen Ungleichung folgt also

$$\frac{y_1^{p/q} + y_2^{p/q} + \dots + y_n^{p/q}}{n} \geq \left(\frac{y_1 + y_2 + \dots + y_n}{n} \right)^{p/q}.$$

Nachdem wir beide Seiten zur $1/p$ -ten Potenz erheben und $y_i = a_i^q$ einsetzen, erhalten wir genau die allgemeine Potenzmittelungleichung. \square

Lösung zu Aufgabe 2 (IMO-Vorauswahl 2012). Betrachte die Funktion $f: \mathbb{R}_{>0} \rightarrow \mathbb{R}$ gegeben durch

$$f(x) = \frac{x+2}{(x+1)(x+5)}.$$

Nach kurzer Rechnung folgt, dass die zweite Ableitung von f wie folgt gegeben ist:

$$f''(x) = \frac{2(x^3 + 6x^2 + 21x + 32)}{(x+1)^3(x+5)^3}.$$

Dieser Ausdruck ist offensichtlich positiv, also ist f in der Tat konvex. Wir wenden jetzt die gewichtete Jensen-Ungleichung mit den Gewichten $a+1$, $b+1$ und $c+1$ an und erhalten:

$$\frac{(a+1)f(b) + (b+1)f(c) + (c+1)f(a)}{a+b+c+3} \geq f\left(\frac{(a+1)b + (b+1)c + (c+1)a}{a+b+c+3}\right).$$

Wir setzen nun $u := a+b+c$ und $v := ab+bc+ca$, sodass $(a+1)b + (b+1)c + (c+1)a = u+v$. Mithilfe der obigen Abschätzung müssen wir also nur

$$(u+3)f\left(\frac{u+v}{u+3}\right) \geq \frac{3}{2}$$

zeigen. Indem wir $(u+v)/(u+3)$ in die Definition von f einsetzen, erhalten wir

$$(u+3)f\left(\frac{u+v}{u+3}\right) = \frac{(u+3)^2(3u+v+6)}{(2u+v+3)(6u+v+15)} = \frac{3}{2} \cdot \frac{(u+3)^2(6u+2v+12)}{(6u+3v+9)(6u+v+15)}.$$

Aus der Voraussetzung $a^2 + b^2 + c^2 \geq 3$ folgt $u^2 - 2v \geq 3$. Also erhalten wir die Abschätzung $(u+3)^2 = u^2 + 6u + 9 \geq 6u + 2v + 12$. Aus der AM-GM-Ungleichung folgt schließlich

$$(6u+2v+12)^2 = \left(\frac{(6u+3v+9) + (6u+v+15)}{2} \right)^2 \geq (6u+3v+9)(6u+v+15).$$

Indem wir alle Abschätzungen bisher kombinieren, erhalten wir

$$(u+3)f\left(\frac{u+v}{u+3}\right) \geq \frac{3}{2} \cdot \frac{(6u+2v+12)^2}{(6u+3v+9)(6u+v+15)} \geq \frac{3}{2}.$$

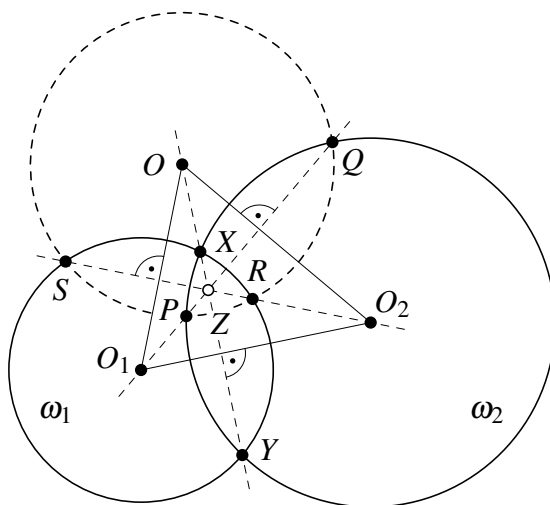
Damit ist die Aufgabe gelöst. \square

Der Trick, einen Teil der Variablen als Funktion und den Rest als Jensen-Gewichte aufzufassen, kommt nicht besonders häufig zum Einsatz, aber ihr solltet ihn in der Hinterhand behalten. Außerdem ist er ziemlich cool.

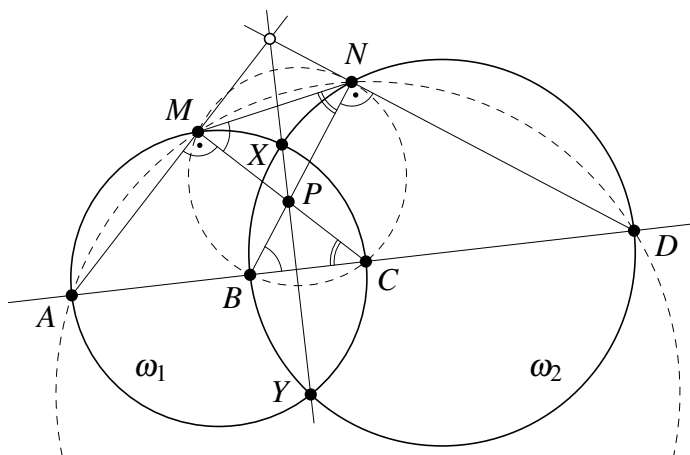
Lösungen zu Kapitel 4: Potenzgeraden

Lösung zu Aufgabe 1 (USAMO 2009/1). Wenn $PQRS$ ein Sehnenviereck ist, dann schneiden sich PQ , RS und XY in einem Punkt Z , denn bei diesen Geraden handelt es sich um die paarweisen Potenzgeraden der Kreise ω_1 , ω_2 und $\odot PQRS$.

Seien nun O_1 , O_2 und O die Mittelpunkte der Kreise ω_1 , ω_2 und $\odot PQRS$. Wenn sich zwei Kreise schneiden, dann steht die Verbindungsgerade ihrer Mittelpunkte stets senkrecht auf der Verbindungsgeraden der beiden Schnittpunkte. Insbesondere steht OO_1 senkrecht auf der Geraden RS . Weil RS nach Annahme durch O_2 verläuft, muss RS also die Höhe durch O_2 im Dreieck OO_1O_2 sein. Analog ist PQ die Höhe durch O_1 . Ihr Schnittpunkt Z ist somit der Höhenschnittpunkt von OO_1O_2 . Folglich muss OZ die Höhe durch O sein. Also steht OZ senkrecht auf O_1O_2 . Die Gerade XY verläuft aber ebenfalls durch Z und steht senkrecht auf O_1O_2 . Folglich müssen die Geraden OZ und XY identisch sein, sodass O auf XY liegt. \square



Lösung zu Aufgabe 2 (IMO 1995/1). Unser Ziel ist zu zeigen, dass $ADNM$ ein Sehnenviereck ist, denn dann handelt es sich bei AM , DN und XY um die paarweisen Potenzgeraden der Kreise ω_1 , ω_2 und $ADNM$, welche sich in einem Punkt schneiden.

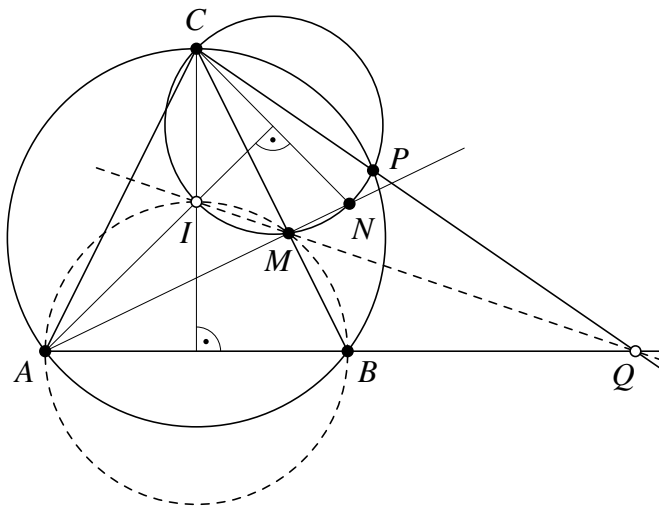


Nach dem Sehnensatz in den Kreisen ω_1 und ω_2 gilt $|CP| \cdot |MP| = |XP| \cdot |YP| = |BP| \cdot |NP|$. Nach der Umkehrung des Sehnensatzes ist $BCNM$ also ein Sehnenviereck. Nach dem Satz des Thales gilt $\sphericalangle AMC = 90^\circ = \sphericalangle BND$. Also ist $\sphericalangle CAM = 180^\circ - \sphericalangle AMC - \sphericalangle MCA = 90^\circ - \sphericalangle MCA$. Nach dem Peripheriewinkelsatz im Sehnenviereck $BCNM$ gilt aber auch $\sphericalangle MCA = \sphericalangle MNB$. Es folgt

$$\sphericalangle DAM + \sphericalangle MND = \sphericalangle CAM + \sphericalangle MNB + \sphericalangle BND = (90^\circ - \sphericalangle MCA) + \sphericalangle MCA + 90^\circ = 180^\circ.$$

Folglich muss $ADNM$ ein Sehnenviereck sein und wir sind fertig. \square

Lösung zu Aufgabe 3 (IMO-Vorauswahl 2012). Sei I der Schnittpunkt der Winkelhalbierenden von $\sphericalangle BMN$ mit der Winkelhalbierenden von $\sphericalangle ACB$. Dann ist I der Inkreismittelpunkt des Dreiecks AMC . Wir werden zeigen, dass $ABMI$ und $CIMN$ Sehnenvierecke sind. Wenn wir das zeigen können, sind wir fertig. Denn dann folgt, dass AB , CP und die Winkelhalbierende von $\sphericalangle BMN$ die paarweisen Potenzgeraden der Kreise $\odot ABC$, $\odot CIMN$ und $\odot ABMI$ sind. Also schneiden sie sich in einem Punkt. Folglich liegt der Schnittpunkt Q von AB und CP auf der Winkelhalbierenden von $\sphericalangle BMN$, wie behauptet.



Gemäß dem Südpolsatz (bzw. in diesem Fall dem „Nordpolsatz“) schneiden sich die Mittelsenkrechte von \overline{CN} und die Außenwinkelhalbierende von $\sphericalangle NMC$ auf dem Umkreis $\odot CMN$. Nach Voraussetzung gilt $|AC| = |AN|$, also ist die Mittelsenkrechte von \overline{CN} auch die Winkelhalbierende von $\sphericalangle MAC$. Ferner ist die Außenwinkelhalbierende von $\sphericalangle NMC$ auch die Winkelhalbierende von $\sphericalangle CMA$. Somit ist der betrachtete Schnittpunkt genau der Inkreismittelpunkt von AMC . Damit haben wir gezeigt, dass I auf dem Umkreis $\odot CMN$ liegt, sodass $CIMN$ ein Sehnenviereck ist.

Nach dem „Nordpolsatz“ schneiden sich außerdem die Mittelsenkrechte von \overline{AB} und die Außenwinkelhalbierende von $\sphericalangle AMB$ auf dem Umkreis $\odot ABM$. Wegen $|AC| = |BC|$ ist die Mittelsenkrechte von \overline{AB} gleichzeitig die Winkelhalbierende von $\sphericalangle ACB$. Ferner ist die Außenwinkelhalbierende von $\sphericalangle AMB$ auch die Winkelhalbierende von $\sphericalangle CMA$. Somit ist I wieder der betrachtete Schnittpunkt. Damit haben wir gezeigt, dass I auf dem Umkreis $\odot ABM$ liegt, sodass $ABMI$ ein Sehnenviereck ist. \square

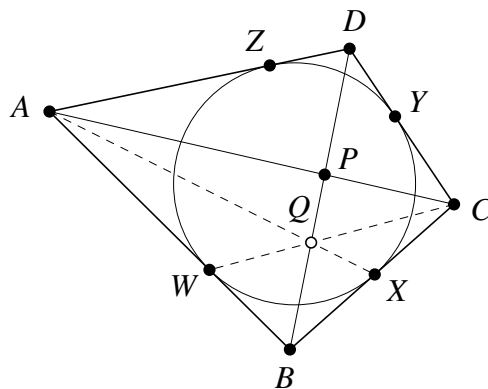
Lösung zu Aufgabe 4. Indem wir den Satz von Brianchon auf das entartete Tangentensechseck $AWBXC D$ anwenden, erhalten wir, dass sich dessen Hauptdiagonalen AX , CW und BD in einem Punkt Q schneiden. Aus dem Satz von Ceva folgt sodann

$$\frac{|AP|}{|CP|} \cdot \frac{|CX|}{|BX|} \cdot \frac{|BW|}{|AW|} = 1.$$

Nun gilt aber auch $|BW| = |BX|$, denn bei den Strecken \overline{BW} und \overline{BX} handelt es sich um die Tangentenabschnitte von B an den Inkreis von $ABCD$. Durch Einsetzen in die obige Gleichung erhalten wir

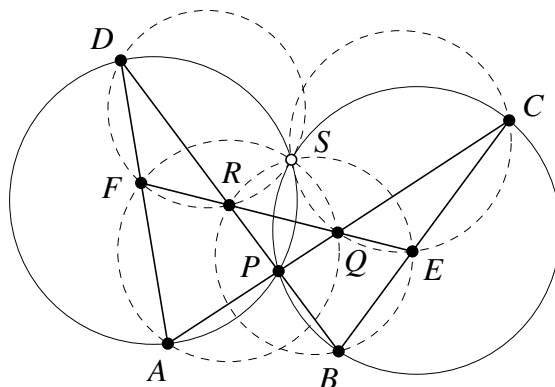
$$\frac{|AP|}{|CP|} \cdot \frac{|CX|}{|AW|} = 1, \quad \text{also} \quad \frac{|AP|}{|CP|} = \frac{|AW|}{|CX|}.$$

Damit ist die erste der gewünschten Verhältnisgleichungen gezeigt. Wieder aufgrund gleich langer Tangentenabschnitte gilt $|AZ| = |AW|$ und $|CY| = |CX|$. Daraus folgt sofort die zweite Verhältnisgleichung. \square



Lösungen zu Kapitel 5: (Dreh-)Streckungen

Lösung zu Aufgabe 1 (IMO 2005/5). Betrachte die Drehstreckung σ um S , die den Umkreis $\odot BCP$ auf den Umkreis $\odot DAP$ abbildet. Wir haben gesehen, dass σ auch als Projektion durch den zweiten Schnittpunkt der Umkreise beschrieben werden kann, also als Projektion durch P . Weil P aber auch der Schnittpunkt von AC und BD ist, folgt $\sigma(C) = A$ und $\sigma(B) = D$. Also bildet σ die Strecke \overline{BC} auf die Strecke \overline{DA} ab. Wegen $|BC| = |DA|$ muss σ somit eine Drehung sein.



Aus $|BE| = |DF|$ folgt nun, dass σ auch die Strecke \overline{BE} auf die Strecke \overline{DF} abbildet. Nach dem gleichen Argument wie für \overline{BC} und \overline{DA} wissen wir aber auch, dass es eine Drehung σ' um den zweiten Schnittpunkt der Umkreise $\odot BER$ und $\odot DFR$ gibt, die \overline{BE} auf \overline{DF} abbildet. Weil orientierungserhaltende Ähnlichkeitstransformationen durch 2 Punkte eindeutig bestimmt sind, muss $\sigma = \sigma'$ gelten. Folglich ist S auch das Zentrum der Drehung σ' und liegt somit auf den Umkreisen $\odot BER$ und $\odot DFR$. Damit ist gezeigt, dass $BERS$ und $DFRS$ Sehnenvierecke sind. Das Argument für $CEQS$ und $AFQS$ geht analog. Damit ist (a) gezeigt.

Für (b) machen wir eine Winkeljagd (und betrachten der Einfachheit halber nur den Lagebeziehungsfall aus der Skizze). Es gilt $\sphericalangle RSQ = \sphericalangle FSQ - \sphericalangle FSR$. Nach dem Peripheriewinkelsatz im Sehnenviereck $FRSD$ gilt $\sphericalangle FSR = \sphericalangle FDR = \sphericalangle ADP$. Andererseits gilt im Sehnenviereck $AQSF$ die Gleichung $\sphericalangle FSQ = 180^\circ - \sphericalangle QAF = 180^\circ - \sphericalangle PAD$. Aus der Innenwinkelsumme im Dreieck APD folgt nun

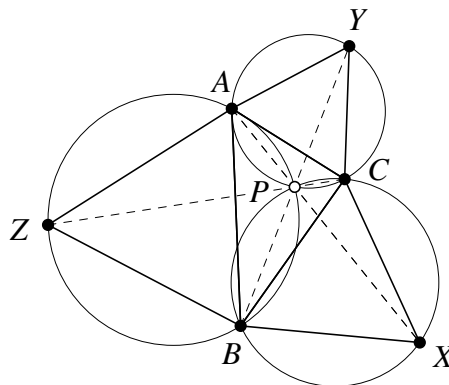
$$\sphericalangle RSQ = \sphericalangle FSQ - \sphericalangle FSR = (180^\circ - \sphericalangle PAD) - \sphericalangle ADP = \sphericalangle DPA = 180^\circ - \sphericalangle QPR.$$

Damit ist $PQRS$ ein Sehnenviereck. □

Lösung zu Aufgabe 2. Sei P der von C verschiedene Schnittpunkt der Umkreise $\odot BXC$ und $\odot CYA$. Dann gilt $\sphericalangle BPC = 180^\circ - 60^\circ = 120^\circ$ und $\sphericalangle CPA = 180^\circ - 60^\circ = 120^\circ$. Es folgt

$$\sphericalangle BZA + \sphericalangle APB = 60^\circ + (360^\circ - 120^\circ - 120^\circ) = 180^\circ.$$

Also ist $AZBP$ ein Sehnenviereck und somit liegt P auch auf dem Umkreis $\odot AZB$. Damit ist (a) bewiesen.

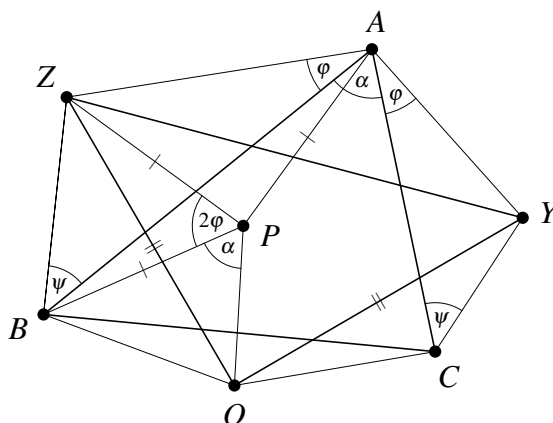


Für (b) betrachte die Drehstreckung σ um A , die Z auf C abbildet. Weil AZB und ACY gleichseitige Dreiecke sind, wird dann auch B auf Y abgebildet. Dann werden auch die Umkreise $\odot AZB$ und $\odot CYA$ aufeinander abgebildet. Folglich lässt sich σ aber auch als Projektion durch den zweiten Schnittpunkt P beschreiben. Wegen $\sigma(Z) = C$ und $\sigma(B) = Y$ muss P also auf BY und auf CZ liegen. Analog liegt P auch auf AX . \square

Lösung zu Aufgabe 3, Aufgabe 4 und zum Satz von Napoleon. Wir beweisen alle drei gleichzeitig, indem wir sie als Spezialfälle aus dem folgenden Master-Lemma folgern. \square

Master-Lemma für aufgesetzte Dreiecke. Sei ABC ein Dreieck. Auf die Seiten \overline{CA} und \overline{AB} werden nach außen Dreiecke CYA und AZB aufgesetzt. Dabei gelte $\sphericalangle CAY = \sphericalangle ZAB =: \varphi$ sowie $\sphericalangle YCA = \sphericalangle ABZ =: \psi$. Ferner sei X ein Punkt, der bezüglich BC in der gleichen Halbebene wie A liegt und für den $\sphericalangle XCB = \sphericalangle ZAB = \varphi$ sowie $\sphericalangle CBX = \sphericalangle ABZ = \psi$ gilt (das Dreieck BCX wird also nicht nach außen aufgesetzt). Sei O der Mittelpunkt des Umkreises $\odot BCX$ und sei P der Mittelpunkt des Umkreises $\odot AZB$. Dann ist das Dreieck OYZ gleichschenkelig mit Spitze O und außerdem ähnlich zum Dreieck PAZ .

Beweis. Betrachte die Drehstreckung σ mit Zentrum Z , die P auf A abbildet. Wenn wir zeigen können, dass $\sigma(O) = Y$ ist, dann folgt wie gewünscht $OYZ \sim PAZ$. Ferner muss das Dreieck PAZ gleichschenkelig mit Spitze P sein, denn P ist der Umkreismittelpunkt von AZB . Folglich wäre auch OYZ gleichschenkelig mit Spitze O und wir wären fertig.



Um $\sigma(O) = Y$ zu zeigen, betrachten wir zunächst die Drehstreckung τ um B , die C auf A abbildet. Weil die Dreiecke BCX und BAZ nach Annahme gleichsinnig ähnlich sind, werden sie unter τ aufeinander abgebildet. Dann werden auch ihre Umkreismittelpunkte P und O aufeinander abgebildet. Aus $\tau(O) = P$ und $\tau(C) = A$ folgt nun, dass BOP und BCA gleichsinnig ähnlich sind. Insbesondere ist $\sphericalangle BPO = \sphericalangle BAC =: \alpha$. Nun gilt $\sphericalangle ZAY = 2\varphi + \alpha$. Nach dem

Betrachte nun die Streckung σ am Berührungspunkt F , die ω auf Ω abbildet. Dann bildet σ auch die Mittelpunkte dieser Kreise aufeinander ab, sodass $\sigma(I) = O$ sein muss. Also bildet σ die Gerade EI auf die Parallele zu EI durch O ab. Aus unserer obigen Beobachtung folgt somit $\sigma(EI) = \ell$. Als Schnittpunkt von EF mit ℓ muss M folglich das Bild von E unter der Streckung σ sein.

Das Bild von AC unter σ ist eine Parallele zu AC , die den Kreis Ω berührt. Weil E auf AC liegt, muss $\sigma(E) = M$ auf $\sigma(AC)$ liegen. Also berührt die Parallele zu AC durch M in der Tat den Kreis Ω . \square

Lösungen zu Kapitel 7: Der Heiratssatz

Lösung zu Aufgabe 1. Wir betrachten einen bipartiten Graphen $G = (A \cup B, E)$, der wie folgt konstruiert ist: A ist die Menge der Schalen und B ist die Menge der Farben. Zwischen $a \in A$ und $b \in B$ verläuft genau dann eine Kante, wenn die Schale a eine Kugel in der Farbe b enthält. Wenn wir ein Matching M konstruieren können, das alle Knoten aus A überdeckt (und damit auch alle Knoten aus B , denn $|A| = n = |B|$), dann sind wir fertig, denn dann können wir aus jeder Schale eine Kugel in der ihr zugeordneten Farbe entnehmen und haben insgesamt jede der n Farben genau einmal abgedeckt.

Wir müssen somit Bedingung des Heiratssatzes prüfen. Sei $S \subseteq A$ eine Teilmenge von Knoten, und seien s_1, \dots, s_k die zugehörigen Schalen (hier ist also $k = |S|$). In diesen k Schalen liegen insgesamt kn Kugeln. Da jede Farbe nur n -mal auftritt, müssen unter diesen kn Kugeln mindestens k Farben vertreten sein. Das heißt aber nichts anderes als $|N_G(S)| \geq k = |S|$, also ist der Heiratssatz anwendbar und wir sind fertig. \square

Lösung zu Aufgabe 2. Um seinen Plan zu verwirklichen, muss Norman n Erdbeeren so auswählen, dass in jeder Zeile und jeder Spalte genau eine dieser Erdbeeren liegt. Betrachte dazu einen bipartiten Graphen $G = (A \cup B, E)$, der wie folgt konstruiert ist: A ist die Menge der Zeilen des Kuchens und B ist die Menge der Spalten des Kuchens. Zwischen $a \in A$ und $b \in B$ verläuft genau dann eine Kante, wenn sich die Zeile a und die Spalte b bei einem Kuchenstück schneiden, auf dem eine positive Anzahl Erdbeeren liegt. Wenn wir in G ein Matching M konstruieren können, das alle Knoten aus A überdeckt (und damit auch alle aus B , denn $|A| = n = |B|$), haben wir die Aufgabe gelöst! Die Kanten aus M bestimmen nämlich n Kuchenstücke, eines in jeder Zeile und Spalte, die jedes mindestens eine Erdbeere enthalten. Dann kann Norman eine Erdbeere von jedem dieser Stücke naschen und damit die gewünschte Bedingung erfüllen.

Nehmen wir also umgekehrt an, es gäbe kein solches Matching M . Nach dem Heiratssatz muss eine nichtleere Teilmenge $S \subseteq A$ existieren, sodass $|N_G(S)| < |S|$. In unser ursprüngliches Problem übersetzt heißt das: Es gibt Zeilen z_1, z_2, \dots, z_k und Spalten s_1, s_2, \dots, s_m , wobei $m < k$, sodass alle Erdbeeren, die sich in den Zeilen z_1, z_2, \dots, z_k befinden, schon in den Spalten s_1, s_2, \dots, s_m enthalten sind. In den Zeilen z_1, z_2, \dots, z_k sind nach Annahme genau $2025k$ Erdbeeren enthalten. Da sich alle diese Erdbeeren auch in den Spalten s_1, s_2, \dots, s_m befinden, die insgesamt genau $2025m$ Erdbeeren enthalten, muss also $2025k \leq 2025m$ gelten. Das widerspricht aber der Annahme $m < k$. \square

Wir befolgen den Ratschlag und lösen die reine Zahlentheorie-Aufgabe 4, bevor wir uns Aufgabe 3 zuwenden.

Lösung zu Aufgabe 4 (IMO-Shortlist 2011/N2). Betrachte $d := \max\{d_1, d_2, \dots, d_9\}$ und wähle $N := d^8 + 1$. Angenommen, für irgendein $n \geq N$ hat $P(n)$ nur Primfaktoren ≤ 20 . Sei $p_i^{e_i}$ die größte Primpotenz, die $n + d_i$ teilt. Weil $n + d_i$ nur durch die acht verschiedenen Primzahlen 2, 3, 5, 7, 11, 13, 17 oder 19 teilbar sein kann, muss $n + d_i$ ein Produkt von höchstens acht Primpotenzen sein. Folglich gilt

$$p_i^{e_i} \geq \sqrt[8]{n + d_i} \geq \sqrt[8]{d^8 + 1} > d.$$

Nach dem Schubfachprinzip muss es ferner zwei Indizes $1 \leq i < j \leq 9$ mit $p_i = p_j$ geben. Sei $p := p_i = p_j$. Dann sind sowohl $n + d_i$ als auch $n + d_j$ durch $p^{\min\{e_i, e_j\}}$ teilbar. Folglich ist auch $|d_i - d_j|$ durch $p^{\min\{e_i, e_j\}}$ teilbar. Nach Annahme gilt $|d_i - d_j| < d < p^{\min\{e_i, e_j\}}$, also kommt nur $d_i = d_j$ in Frage. Das widerspricht jedoch der Annahme, dass d_1, d_2, \dots, d_9 paarweise verschieden sind. \square

Lösung zu Aufgabe 3. Wir führen die Aufgabe zuerst auf ein Matching-Problem zurück. Wir konstruieren einen bipartiten Graphen $G = (A \cup B, E)$ wie folgt: A ist die Menge aller Zahlen $N + 1, N + 2, \dots, N + n$ und B ist die Menge aller Primzahlen, die eine der Zahlen $N + 1, N + 2, \dots, N + n$ teilen. Zwischen $a \in A$ und $b \in B$ verläuft genau dann eine Kante, wenn a durch die Primzahl b teilbar ist. Um die Aufgabe zu lösen, müssen wir in G ein Matching M konstruieren, das alle Knoten aus A enthält, denn dann können wir jedem $N + i$ eine Primzahl $p_i \mid N + i$ zuordnen, sodass $p_i \neq p_j$ für $i \neq j$.

Angenommen, das wäre unmöglich. Nach dem Heiratssatz muss also eine Menge $S \subseteq A$ mit $|N_G(S)| < |S|$ existieren. In unser ursprüngliches Problem übersetzt heißt das: Es gibt ganze Zahlen $1 \leq i_1 < i_2 < \dots < i_k \leq n$, sodass höchstens $k - 1$ verschiedene Primzahlen existieren, die irgendeine der Zahlen $N + i_1, N + i_2, \dots, N + i_k$ teilen. Für alle $j = 1, 2, \dots, k$ sei $q_j^{e_j}$ die größte Primpotenz, die $N + i_j$ teilt. Nach Annahme kann $N + i_j$ durch höchstens $k - 1 \leq n - 1$ verschiedene Primzahlen teilbar sein, ist also ein Produkt von höchstens $n - 1$ Primpotenzen. Wegen $N \geq n^{n-1}$ folgt daraus

$$q_j^{e_j} > n \quad \text{für alle } j = 1, 2, \dots, k.$$

Andererseits gibt es höchstens $k - 1$ verschiedene Primzahlen, die überhaupt irgendeine der Zahlen $N + i_1, N + i_2, \dots, N + i_k$ teilen. Nach dem Schubfachprinzip muss es also Indizes $j \neq \ell$ geben, für die $q_j = q_\ell$ gilt. Sei $q := q_j = q_\ell$. Dann sind sowohl $N + i_j$ als auch $N + i_\ell$ durch $q^{\min\{e_j, e_\ell\}}$ teilbar. Folglich ist $|i_j - i_\ell|$ ebenfalls durch $q^{\min\{e_j, e_\ell\}}$ teilbar. Nun gilt aber auch $|i_j - i_\ell| < n < q^{\min\{e_j, e_\ell\}}$, also kommt nur $i_j = i_\ell$ in Frage. Das widerspricht jedoch unserer Annahme $j \neq \ell$. \square

Lösung zu Aufgabe 5 (IMO-Shortlist 2012/C5). Wir konstruieren einen bipartiten Graphen $G = (A \cup A', E)$ wie folgt: A ist die Menge aller Azur-farbenen Spielsteine und A' ist die Menge aller Azur-farbenen Felder. Zwischen $a \in A$ und $a' \in A'$ verläuft genau dann eine Kante, wenn der Abstand zwischen dem Feld, auf dem a steht, und dem Feld a' maximal $d + 2$ beträgt. Wenn wir in G ein Matching M konstruieren können, das alle Knoten aus A überdeckt (und damit auch alle aus A' , denn $|A| = 3n^2 = |A'|$), dann haben gezeigt, dass alle Azur-farbenen Spielsteine wie gewünscht verschoben werden können. Mit einem analogen Argument für die Farben Bordeaux und Citrin haben wir dann die Aufgabe gelöst.

Betrachte eine Menge $S \subseteq A$ von Azur-farbenen Spielsteinen. Für alle positiven reellen Zahlen r sei S_r die Menge aller Felder, die höchstens Abstand r von einem Feld haben, auf dem ein Spielstein aus S steht. Um die Bedingung des Heiratssatzes zu überprüfen, müssen wir zeigen, dass es in S_{d+2} mindestens $|S|$ Azur-farbene Felder gibt. Intuitiv ist das sehr plausibel: Einerseits ist durchschnittlich ein Drittel aller Felder Azur-farben, also können wir annehmen, dass $\approx \frac{1}{3}|S_{d+2}|$ Felder in S_{d+2} Azur-farben sind. Andererseits muss es in S_d mindestens $|S|$ Bordeaux- und mindestens $|S|$ Citrin-farbene Felder geben, denn nach Annahme existiert eine Permutation der Spielsteine, die jeden Spielstein maximal im Abstand d bewegt und Azur auf Bordeaux, Bordeaux auf Citrin und Citrin auf Azur schickt. Somit ist $3|S| \leq |S_d|$. Wegen $S_d \subseteq S_{d+2}$ erhalten wir also $|S| \lesssim \frac{1}{3}|S_{d+2}|$.

Der formale Beweis ist nicht viel schwieriger. Wir können das $3n \times 3n$ -Feld mit horizontalen 3×1 -Rechtecken parkettieren, sodass in jedem dieser Rechtecke jede Farbe mindestens einmal vertreten ist. Wenn R ein solches 3×1 -Rechteck ist und ein Feld von R in S_d enthalten ist, dann

sind alle drei Felder in S_{d+2} enthalten. Somit enthält S_{d+2} mindestens $\frac{1}{3}|S_d|$ Azur-farbene Felder. Das ist genau die Abschätzung, die wir brauchen, um die obigen Plausibilitätsüberlegungen wasserdicht zu machen. \square

Lösungen zu Kapitel 8: Multiplikative Ordnungen und Primitivwurzeln

Lösung zu Aufgabe 1. Es gilt $a^n \equiv 1 \pmod{a^n - 1}$ und $1 < a^i < a^n - 1$ für alle $i = 1, 2, \dots, n-1$. Folglich ist $n = \text{ord}_{a^n-1}(a)$. Weil $\text{ord}_{a^n-1}(a)$ ein Teiler von $\varphi(a^n - 1)$ sein muss, folgt die Behauptung. \square

Lösung zu Aufgabe 2. Wir beginnen mit (a). Wenn q ein Primteiler von $\frac{n^p-1}{n-1}$ ist, dann gilt $n^p \equiv 1 \pmod{q}$. Also ist $\text{ord}_q(n)$ ein Teiler von p . Weil p eine Primzahl ist, kommen nur $\text{ord}_q(n) = 1$ und $\text{ord}_q(n) = p$ in Frage. Im ersten Fall gilt $n \equiv 1 \pmod{q}$, also auch

$$0 \equiv \frac{n^p - 1}{n - 1} \equiv 1 + n + \dots + n^{p-1} \equiv \underbrace{1 + 1 + \dots + 1}_{p \text{ Summanden}} \equiv p \pmod{q}.$$

Somit muss $p = q$ gelten. Im zweiten Fall folgt $q \equiv 1 \pmod{p}$ aus der Tatsache, dass $\text{ord}_q(n)$ stets ein Teiler von $\varphi(q) = q - 1$ ist.

Für Teil (b) nehmen wir an, dass wir schon m Primzahlen q_1, q_2, \dots, q_m mit $q_i \equiv 1 \pmod{p}$ für alle $i = 1, 2, \dots, m$ gefunden haben. Betrachte $n := pq_1q_2 \dots q_m$. Dann ist $\frac{n^p-1}{n-1} = 1 + n + \dots + n^{p-1}$ durch keine der Primzahlen p, q_1, q_2, \dots, q_m teilbar. Nach (a) erfüllt dann jeder Primfaktor q von $\frac{n^p-1}{n-1}$ die Kongruenz $q \equiv 1 \pmod{p}$. Somit haben wir mindestens eine weitere Primzahl mit der gewünschten Eigenschaft gefunden. \square

Lösung zu Aufgabe 3 (IMO 1999/4). Offensichtlich ist $(n, p) = (1, p)$ eine Lösung für jede Primzahl p .

Ab jetzt betrachten wir nur noch den Fall $n \geq 2$. Sei q der kleinste Primfaktor von n . Aus $n^{p-1} \mid (p-1)^n + 1$ folgt $(p-1)^n \equiv -1 \pmod{q}$, also $(p-1)^{2n} \equiv 1 \pmod{q}$. Somit ist $\text{ord}_q(p-1)$ ein Teiler von $2n$. Aber $\text{ord}_q(p-1)$ ist auch ein Teiler von $\varphi(q) = q - 1$. Nun sind n und $q - 1$ teilerfremd (sonst hätte n noch einen kleineren Primfaktor). Also kommen nur $\text{ord}_q(p-1) = 1$ oder $\text{ord}_q(p-1) = 2$ in Frage.

Fall 1: Es gilt $\text{ord}_q(p-1) = 1$. Dann ist $p-1 \equiv 1 \pmod{q}$. Wegen $(p-1)^n \equiv -1 \pmod{q}$ kann nur $q = 2$ sein. Wenn $p \geq 3$ eine ungerade Primzahl ist, dann ist $(p-1)^n + 1$ ungerade und kann nicht durch $q = 2$ teilbar sein. Also kommt nur $p = 2$ in Frage. In diesem Fall ist $(p-1)^n + 1 = 2$ und $n^{p-1} = n$ muss ein Teiler von 2 sein. Also kommt nur $n = 2$ in Frage. Tatsächlich ist $(n, p) = (2, 2)$ eine Lösung.

Fall 2: Es gilt $\text{ord}_q(p-1) = 2$. Dann gilt $(p-1)^2 \equiv 1 \pmod{q}$, aber $p-1 \not\equiv 1 \pmod{q}$. Das Polynom $X^2 - 1$ hat modulo q genau die Nullstellen $X = \pm 1$, denn es lässt sich zu $(X-1)(X+1)$ faktorisieren. Somit kommt nur $p-1 \equiv -1 \pmod{q}$ in Frage. Dann ist aber $p \equiv 0 \pmod{q}$, also $p = q$. Nun ist n durch q teilbar und es gilt $n \leq 2p = 2q$, also gibt es nur die Möglichkeiten $n = q$ und $n = 2q$. Im zweiten Fall muss $q = 2$ sein, denn sonst wäre q nicht der kleinste Primfaktor von n . Es folgt also $(n, p) = (2q, q) = (4, 2)$, aber das ist offensichtlich keine Lösung. Somit muss $n = p = q$ sein. Wir müssen folglich herausfinden, für welche Primzahlen $(p-1)^p + 1$ durch p^{p-1} teilbar ist. Den Fall $p = 2$ haben wir in Fall 1 bereits betrachtet. Also dürfen wir $p \geq 3$ annehmen. Nun betrachten wir $(p-1)^p + 1$ modulo p^3 : Es gilt

$$(p-1)^p + 1 \equiv \sum_{k=0}^p \binom{p}{k} p^k (-1)^{p-k} + 1 \equiv 1 - \binom{p}{1} p + 1 \equiv -p^2 \pmod{p^3}.$$

Hier haben wir benutzt, dass alle Summanden für $k \geq 3$ durch p^3 teilbar sind. Der Summand für $k = 2$ ist ebenfalls durch p^3 teilbar, denn der Binomialkoeffizient $\binom{p}{2} = \frac{(p-1)p}{2}$ ist für ungerade Primzahlen p stets durch p teilbar. Wir sehen also, dass $(p-1)^p + 1$ nicht durch p^3 teilbar sein. Also ist $p = 3$ die einzige ungerade Primzahl, für die $p^{p-1} \mid (p-1)^p + 1$ gelten kann. Es ist leicht nachzuprüfen, dass $(n, p) = (p, p) = (3, 3)$ tatsächlich eine Lösung ist.

Weil die Fallunterscheidung vollständig ist, haben wir damit alle Lösungen gefunden. \square

Lösung zu Aufgabe 4 (Chinesische MO 2009/2). Wir betrachten drei Fälle:

Fall 1: Es gilt $p = 5$. Dann ist p auf jeden Fall ein Teiler von $5^p + 5^q$. Nach dem kleinen Satz von Fermat gilt ferner $5^q \equiv 5 \pmod{q}$. Folglich ist q genau dann ein Teiler von $5^p + 5^q$, wenn $0 \equiv 5^p + 5^q \equiv 5^5 + 5 \pmod{q}$ gilt. Wegen $5^5 + 5 = 2 \cdot 5 \cdot 313$ liefert das die drei Lösungen $(p, q) = (5, 2)$, $(p, q) = (5, 5)$ und $(p, q) = (5, 313)$.

Fall 2: Es gilt $q = 5$. Analog zu Fall 1 erhalten wir die drei Lösungen $(p, q) = (2, 5)$, $(p, q) = (5, 5)$ und $(p, q) = (313, 5)$.

Fall 3: Es gilt $p, q \neq 5$. Nach dem kleinen Satz von Fermat gilt $5^p \equiv 5 \pmod{p}$. Damit p ein Teiler von $5^p + 5^q$ gilt, muss also $5 + 5^q \equiv 0 \pmod{p}$ sein. Wegen $p \neq 5$ folgt $5^{q-1} \equiv -1 \pmod{p}$ und somit $5^{2(q-1)} \equiv 1 \pmod{p}$. Somit ist $\text{ord}_p(5)$ ein Teiler von $2(q-1)$, aber kein Teiler von $q-1$. Andererseits ist $\text{ord}_p(5)$ stets ein Teiler von $p-1$. Also muss $p-1$ mindestens einmal mehr durch 2 teilbar sein als $q-1$. Das gleiche Argument lässt sich aber auch umgekehrt durchführen und wir erhalten, dass $q-1$ mindestens einmal mehr durch 2 teilbar sein muss als $p-1$. Das ist ein Widerspruch! \square

Lösung zu Aufgabe 5 (Rumänische IMO-Auswahl 2009). Sei $r > 3$ eine Primzahl, sei p ein Primfaktor von $2^r - 1$ und sei q ein Primfaktor von $2^r + 1$. Dann ist $2^r \equiv 1 \pmod{p}$, also ist $\text{ord}_p(2)$ ein Teiler von r . Weil r eine Primzahl ist, kommt nur $\text{ord}_p(2) = 1$ oder $\text{ord}_p(2) = r$ in Frage. Ersterer Fall ist offensichtlich unmöglich, denn er führt auf $2 \equiv 1 \pmod{p}$. Also muss $\text{ord}_p(2) = r$ gelten.

Wir würden gern analog $\text{ord}_q(2) = 2r$ folgern. Um das tun zu können, bemerken wir zunächst, dass wir stets $q > 3$ wählen können. Ansonsten müsste $2^r + 1$ nämlich eine Dreierpotenz sein, was für $r > 3$ nicht der Fall ist. Das lässt sich zum Beispiel durch geschickte Faktorisierung zeigen (dafür brauchen wir noch nicht mal, dass r prim ist). Hier präsentieren wir stattdessen ein Overkill-Argument mit Ordnungen: Aus $2^r + 1 = 3^n$ folgt $2^{2r} \equiv 1 \pmod{3^n}$. Also ist $\text{ord}_{3^n}(2)$ ein Teiler von $2r$, aber auch ein Teiler von $\varphi(3^n) = 2 \cdot 3^{n-1}$. Wegen $r > 3$ kommen nur $\text{ord}_{3^n}(2) = 1$ oder $\text{ord}_{3^n}(2) = 2$ in Frage. Der erste Fall ist nur für $2 \equiv 1 \pmod{3^n}$, also nur für $n = 0$ möglich, und der zweite Fall nur für $2^2 \equiv 1 \pmod{3^n}$, also nur für $n = 0$ oder $n = 1$. In jedem Fall sehen wir, dass $2^r + 1 = 3^n$ für $r > 3$ nicht möglich ist.

Weil q ein Teiler von $2^r + 1$ ist, folgt $2^{2r} \equiv 1 \pmod{q}$. Somit ist $\text{ord}_q(2)$ ein Teiler von $2r$. Es ergeben sich die Möglichkeiten $\text{ord}_q(2) = 1$, $\text{ord}_q(2) = 2$, $\text{ord}_q(2) = r$ und $\text{ord}_q(2) = 2r$. Die ersten beiden Fälle sind für $q > 3$ unmöglich und der dritte Fall ist unmöglich, weil in unserem Fall $2^r \equiv -1 \not\equiv 1 \pmod{q}$ gilt. Es verbleibt $\text{ord}_q(2) = 2r$, wie behauptet.

Andererseits ist $\text{ord}_p(2)$ ein Teiler von $p-1$ und $\text{ord}_q(2)$ ein Teiler von $q-1$. Folglich erhalten wir $p \equiv 1 \pmod{r}$ und $q \equiv 1 \pmod{2r}$. Weil $p-1$ gerade ist, muss sogar $p \equiv 1 \pmod{2r}$ sein. Es folgt, dass $p-1$ durch $\text{ord}_q(2) = 2r$ teilbar ist, sodass $q \mid 2^{p-1} - 1$. Ebenso ist $q-1$ durch $\text{ord}_p(2) = r$ teilbar, sodass $p \mid 2^{q-1} - 1$. Damit haben wir ein Paar von Primzahlen mit der gewünschten Eigenschaft konstruiert. Weil $2^r - 1$ und $2^r + 1$ teilerfremd sind, muss ferner $p \neq q$ gelten, wie gewünscht.

Um zu zeigen, dass unendlich viele solche Paare existieren, nehmen wir an, dass wir bereits Paare $(p_1, q_1), (p_2, q_2), \dots, (p_m, q_m)$ konstruiert haben. Indem wir die obige Konstruktion mit einer Primzahl $r > \max\{p_1, p_2, \dots, p_m, q_1, q_2, \dots, q_m\}$ durchführen, erhalten wir Primzahlen p

und q mit $p, q \equiv 1 \pmod{2r}$. Folglich sind p und q verschieden von allen bisher konstruierten Primzahlen und wir haben ein weiteres Paar mit den gewünschten Eigenschaften konstruiert. \square

Lösungen zu Kapitel 9: Quadratische Reste

Lösung zu Aufgabe 1. Wir beginnen mit (a). Angenommen, wir haben schon m Primzahlen p_1, p_2, \dots, p_m mit $p_i \equiv 3 \pmod{m}$ für alle $i = 1, 2, \dots, m$ gefunden. Wir werden zeigen, dass stets eine weitere solche Primzahl existiert. Betrachte dazu $N := 4p_1p_2 \cdots p_m - 1$. Dann ist $N \equiv 3 \pmod{4}$, also kann es nicht sein, dass alle Primfaktoren $p \mid N$ von der Form $p \equiv 1 \pmod{4}$ sind. Wir finden somit eine Primzahl $p \mid N$ mit $p \equiv 3 \pmod{4}$. Andererseits ist N teilerfremd zu p_1, p_2, \dots, p_m . Also haben wir mit p eine weitere Primzahl konstruiert, die die gewünschte Eigenschaft erfüllt.

Der Beweis für (b) geht analog, nur dass wir hier $N := (2p_1p_2 \cdots p_m)^2 + 1$ betrachten. Dann ist N ungerade und zu p_1, p_2, \dots, p_m teilerfremd. Ferner muss -1 für jeden Primteiler $p \mid N$ ein quadratischer Rest modulo p sein. Nach dem ersten Ergänzungssatz zum QRG muss dafür $p \equiv 1 \pmod{4}$ gelten. Damit haben wir eine weitere Primzahl mit der gewünschten Eigenschaft konstruiert. \square

Lösung zu Aufgabe 2 (IMO 1996/4). Schreibe $15a + 16b = m^2$ und $16a - 15b = n^2$. Dann gilt

$$16m^2 - 15n^2 = 16 \cdot 15a + 16^2b - 15 \cdot 16a + 15^2b = 481b$$

$$15m^2 + 16n^2 = 15^2a + 15 \cdot 16b + 16^2a - 16 \cdot 15b = 481a.$$

Aus $481 = 13 \cdot 37$ folgt nun $16m^2 \equiv 15n^2 \pmod{13}$ und $16m^2 \equiv 15n^2 \pmod{37}$. Wir werden zeigen, dass das nur sein kann, wenn m und n durch 481 teilbar sind. Dazu berechnen wir zuerst das Legendre-Symbol $\left(\frac{15}{13}\right)$: Nach Multiplikativität des Legendre-Symbols und unter Ausnutzung des QRG gilt

$$\left(\frac{15}{13}\right) = \left(\frac{3}{13}\right)\left(\frac{5}{13}\right) = \left(\frac{13}{3}\right)\left(\frac{13}{5}\right) = \left(\frac{1}{3}\right)\left(\frac{3}{5}\right) = -1.$$

Es folgt

$$\left(\frac{16m^2}{13}\right) = \left(\frac{15n^2}{13}\right) = \left(\frac{15}{13}\right)\left(\frac{n^2}{13}\right) = -\left(\frac{n^2}{13}\right).$$

Andererseits sind $16m^2$ und n^2 notwendigerweise quadratische Reste modulo 13. Die einzige Möglichkeit ist also $\left(\frac{16m^2}{13}\right) = 0 = \left(\frac{n^2}{13}\right)$, sodass m und n durch 13 teilbar sein müssen. Mit einem völlig analogen Argument sehen wir, dass m und n auch durch 37 teilbar sein müssen. Wenn m und n positiv sind, muss also $m^2, n^2 \geq 481^2 = 231361$ gelten.

Andererseits ist $m^2 = n^2 = 481^2$ tatsächlich möglich, denn in diesem Fall führen die Gleichungen $16m^2 - 15n^2 = 481b$ und $15m^2 + 16n^2 = 481a$ auf die ganzzahligen Lösungen $a = 481$ und $b = (15 + 16) \cdot 481 = 14911$. \square

Lösung zu Aufgabe 3. Wir zeigen zuerst, dass die Gleichung $a^2 + 5 = b^3$ keine ganzzahligen Lösungen hat. Dazu bemerken wir zunächst, dass b ungerade ist. Sonst wäre nämlich $a^2 + 5 \equiv 0 \pmod{8}$, was unmöglich ist. Als nächstes schreiben wir die Gleichung in der Form

$$a^2 + 4 = b^3 - 1 = (b - 1)(b^2 + b + 1).$$

Für jeden Primfaktor p von $b^2 + b + 1$ folgt dann $a^2 \equiv -4 \pmod{p}$, sodass -4 ein quadratischer Rest modulo p sein muss. Da b ungerade ist, muss $b^2 + b + 1$ ebenfalls ungerade sein, also ist auch jeder Primfaktor p ungerade. Ferner ist $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{4}{p}\right) = \left(\frac{-1}{p}\right)$, denn 4 ist offensichtlich

ein quadratischer Rest modulo p . Folglich ist -4 genau dann ein quadratischer Rest, wenn -1 ein quadratischer Rest ist, also genau dann, wenn $p \equiv 1 \pmod{4}$.

Weil jeder Primfaktor von $b^2 + b + 1$ von der Form $p \equiv 1 \pmod{4}$ ist, muss $b^2 + b + 1 \equiv 1 \pmod{4}$ gelten. Durch Ausprobieren aller Reste modulo 4 folgt daraus $b \equiv 3 \pmod{4}$. Indem wir die ursprüngliche Gleichung modulo 4 betrachten, erhalten wir $a^2 + 5 \equiv b^3 \equiv 3 \pmod{4}$. Daraus folgt nun aber $a^2 \equiv 2 \pmod{4}$, was unmöglich ist.

Auf ähnliche Weise lässt sich zeigen, dass $a^2 + 3 = b^3$ keine ganzzahligen Lösungen hat. Wir bemerken zunächst, dass b ungerade ist. Sonst wäre $a^2 + 3 \equiv 0 \pmod{8}$, was unmöglich ist. Als nächstes schreiben wir die Gleichung in der Form

$$a^2 + 4 = b^3 + 1 = (b + 1)(b^2 - b + 1).$$

Dann ist -4 ein quadratischer Rest modulo jedem Primteiler p von $b^2 - b + 1$. Analog zum obigen Argument folgt dann $p \equiv 1 \pmod{4}$ und somit auch $b^2 - b + 1 \equiv 1 \pmod{4}$. Durch Ausprobieren aller Reste modulo 4 folgt dann $b \equiv 1 \pmod{4}$.

Andererseits können wir die gegebene Gleichung auch in der Form

$$a^2 + 2 = b^3 - 1 = (b - 1)(b^2 + b + 1)$$

schreiben. Dann muss -2 ein quadratischer Rest modulo jedem Primteiler p von $b^2 + b + 1$ sein. Weil b ungerade ist, muss auch $b^2 + b + 1$ ungerade sein. Aus den beiden Ergänzungssätzen zum QRG folgt: Für eine ungerade Primzahl $p \geq 3$ ist -2 genau dann ein quadratischer Rest, wenn $p \equiv 1 \pmod{8}$ oder $p \equiv 3 \pmod{8}$. Als Produkt solcher Primfaktoren muss auch $b^2 + b + 1$ den Rest 1 oder 3 modulo 8 lassen. Wegen $b \equiv 1 \pmod{4}$ gilt aber auch $b^2 + b + 1 \equiv 3 \pmod{4}$, sodass $b^2 + b + 1 \equiv 3 \pmod{8}$ sein muss. Durch Ausprobieren aller Reste modulo 8 folgt nun $b \equiv 1 \pmod{8}$. Indem wir die ursprüngliche Gleichung modulo 8 betrachten, erhalten wir jetzt jedoch $a^2 + 3 \equiv b^3 \equiv 1 \pmod{8}$, also $a^2 \equiv 6 \pmod{8}$, was unmöglich ist. \square

Lösung zu Aufgabe 4 (Polnische MO 2019/2). Der Fall $p = 2$ ist trivial, denn alle Reste modulo 2 sind quadratische Reste. Im Folgenden nehmen wir an, dass p eine ungerade Primzahl ist.

Die Bedingung $r^7 \equiv 1 \pmod{p}$ impliziert $\text{ord}_p(r) = 1$ oder $\text{ord}_p(r) = 7$. Der erste Fall führt auf $r \equiv 1 \pmod{p}$. Folglich ist $r + 1 \equiv r^2 + 1 \equiv r^3 + 1 \pmod{p}$ und die Behauptung gilt offensichtlich. Von nun an nehmen wir $\text{ord}_p(r) = 7$ an. Insbesondere muss $p \equiv 1 \pmod{7}$ sein. Wegen

$$r^7 - 1 = (r - 1)(r^6 + r^5 + r^4 + r^3 + r^2 + r + 1)$$

muss in diesem Fall $r^6 + r^5 + r^4 + r^3 + r^2 + r + 1 \equiv 0 \pmod{p}$ gelten. Andererseits ist

$$(r + 1)(r^2 + 1)(r^3 + 1) \equiv r^6 + r^5 + r^4 + 2r^3 + r^2 + r + 1 \equiv r^3 \pmod{p}.$$

Nun ist r^3 ein quadratischer Rest modulo p . Denn wenn g eine Primitivwurzel modulo p ist und $r \equiv g^n \pmod{p}$, dann folgt aus $r^7 \equiv 1 \pmod{p}$, dass n ein Vielfaches von $\frac{p-1}{7}$ sein muss. Weil p eine ungerade Primzahl ist und $p \equiv 1 \pmod{7}$ gilt, muss $\frac{p-1}{7}$ eine gerade Zahl sein. Damit ist auch n gerade. Folglich ist $r^3 \equiv g^{3n} \pmod{p}$ ein quadratischer Rest, wie behauptet. Es folgt

$$\left(\frac{r+1}{p}\right)\left(\frac{r^2+1}{p}\right)\left(\frac{r^3+1}{p}\right) = \left(\frac{(r+1)(r^2+1)(r^3+1)}{p}\right) = \left(\frac{r^3}{p}\right) = 1.$$

Weil $r + 1$ und $r^2 + 1$ quadratische Reste sind, kommt nur $\left(\frac{r^3+1}{p}\right) = 1$ in Frage, sodass auch $r^3 + 1$ ein quadratischer Rest modulo p sein muss. \square

MatBoj-Regeln

MatBoj – abgeleitet aus dem Russischen – steht für „mathematischer Kampf“.

Zwei Teams lösen Aufgaben und präsentieren anschließend ihre Lösungen.

Phase 1: Das Lösen der Aufgaben

Jede Mannschaft gibt sich einen Namen und wählt einen Mannschaftskapitän und einen Stellvertreter. Diese vertreten die Mannschaft als Sprecher. Nur sie können für die Mannschaft verbindliche Entscheidungen verkünden.

Beide Teams erhalten den gleichen Satz von Aufgaben. Ihnen steht eine vorher bekanntgegebene Zeit zur Verfügung, um die Aufgaben getrennt voneinander zu lösen.

Sollte einem Teammitglied eine Aufgabe bereits bekannt sein, so ist es aus Fairnessgründen dazu aufgefordert, dies der Jury bekanntzumachen (eventuell wird die betreffende Aufgabe durch eine neue ersetzt).

Phase 2: Das Vorstellen der Lösungen

- Den beiden Kapitänen wird gleichzeitig eine leichte Einstiegsaufgabe gestellt, die sie ohne Hilfsmittel lösen müssen. Keines der anderen Teammitglieder darf ihnen dabei helfen. Wer die richtige Antwort gibt, gewinnt für sein Team das Recht zu entscheiden, welches Team als erstes herausfordert. Gibt einer der Kapitäne eine falsche Antwort, erhält das Team des anderen Kapitäns dieses Recht.
- **Herausfordern:** Das entsprechende Team fordert vom gegnerischen Team eine Aufgabe. Das herausgeforderte Team kann die Herausforderung annehmen oder ablehnen:
 - Die *Herausforderung wird angenommen*: Das herausgeforderte Team entsendet ein Teammitglied als *Referenten*, der eine Lösung der Aufgabe vorstellt, das herausfordernde Team entsendet einen *Kritiker*, der Lücken in der Lösung zu finden versucht. Nach der Vorstellung der Lösung darf der Kritiker erst Verständnisfragen stellen und dann die vorgetragene Lösung kritisieren und die von ihm aufgedeckten Lücken füllen. Hilfe aus dem Team ist unzulässig.
 - Die *Herausforderung wird abgelehnt*: Das herausfordernde Team entsendet ein Teammitglied, das eine Lösung der Aufgabe vorstellt, das herausgeforderte Team entsendet einen Kritiker, der Lücken in der Lösung zu finden versucht. Nach der Vorstellung der Lösung darf der Kritiker erst Verständnisfragen stellen und dann die vorgetragene Lösung kritisieren. Er darf jedoch keine von ihm aufgedeckten Lücken füllen. Hilfe aus dem Team ist unzulässig.
- **Bewertung:** Jede Aufgabe ist 12 Punkte wert. Der Referent erhält eine der Punktzahlen 0, 2, 4, 6, 8, 10, 12, je nachdem, wie richtig und vollständig die von ihm vorgetragene Lösung ist. Der Kritiker erhält für das Aufdecken der Lücken in der vorgetragenen Lösung und für das Füllen dieser Lücken jeweils die Hälfte der noch nicht vergebenen Punkte. Wie weit Referent und Kritiker ihren Aufgaben im Einzelnen gerecht wurden, liegt im Ermessen der Jury.
- **Invalid challenge:** Wird die Herausforderung abgelehnt und kann das herausfordernde Team keine Lösung präsentieren, liegt ein *invalid challenge* vor. Die Einschätzung, ob es sich um eine Lösung handelt, liegt im Ermessen der Jury.

In diesem Fall erhält das herausgeforderte Team 6 Punkte.

- Die *nächste Herausforderung*: Es wird abwechselnd herausgefordert. Liegt ein invalid challenge vor, muss das herausfordernde Team erneut eine Aufgabe fordern.
- Die Endphase des Wettbewerbs: Zu einem beliebigen Zeitpunkt kann jedes der beiden Teams beschließen, keine Lösungen mehr zu präsentieren. Das betreffende Team muss aber weiter Kritiker entsenden, da das andere Team solange weiter Lösungen vorstellen kann, wie es will. Die Kritiker dürfen in dieser Endphase des Wettbewerbs nur noch Lücken in den vorgetragenen Lösungen aufzeigen, aber nicht mehr füllen.
- Am Ende des Wettbewerbs muss jedes Teammitglied mindestens einmal als Referent bzw. als Kritiker entsandt worden sein.
- **Time-Out**: Jedes Team hat dreimal im ganzen Wettbewerb die Möglichkeit, ein Time-Out (1 Minute) zu fordern. In dieser Zeit dürfen sich die Repräsentanten beider Teams mit ihren Teammitgliedern absprechen und auch ausgewechselt werden.
- Am Ende des MatBojs gewinnt das Team mit der größeren Punktsomme.

Notizen: