

# Zirkelskript

Leipziger Schülersgesellschaft für Mathematik

Klassenstufe 9/10  
Schuljahr 2009/2010

Christoph Schulze

# 1 Zirkel 02.09.2009

Thema: Wiederholung der Grundlagen der Geometrie - Abbildungen, Kongruenz und Ähnlichkeit, Winkel an Parallelen, Innenwinkelsatz, Kreisgeometrie

- Ähnlichkeitsabbildungen:

- Streckungen
- Kongruenzabbildungen
  - \* Verschiebungen
  - \* Drehungen
  - \* Achsenspiegelungen (Orientierung bleibt nicht erhalten)
  - \* Kombinationen von Verschiebungen, Drehungen und Achsenspiegelungen
    - ⇒ Längenerhaltung, geometrische Objekte sind deckungsgleich

⇒ Winkelerhaltung, Längenverhältniserhaltung, stetige Abbildungen, Flächeninhaltsverhältnis ist quadratisch, Inzidenzerhaltung (Schnitte geometrischer Figuren bleiben), geometrische Objekte gehen in ähnliche geometrische Objekte über (Geraden, Kreise, n-Ecke, Ellipsen ... bleiben erhalten), Aneinandergrenzen, ...

**Definition 1 (Kongruenz).** Zwei geometrische Objekte heißen genau dann zueinander kongruent, wenn sie durch Kongruenzabbildungen aufeinander abgebildet werden können.

**Definition 2 (Ähnlichkeit).** Zwei geometrische Objekte heißen genau dann zueinander ähnlich, wenn sie durch Ähnlichkeitsabbildungen aufeinander abgebildet werden können.

**Satz 1 (Kongruenzsätze für Dreiecke).** Zwei Dreiecke sind genau dann kongruent, wenn sie:

- in ihren drei Seiten übereinstimmen (SSS)
- in zwei Seiten und ihrem eingeschlossenen Winkel übereinstimmen (SWS)
- in zwei Seiten und dem Winkel gegenüber der größeren Seite übereinstimmen (SsW)
- in einer Seite und zwei Winkeln übereinstimmen (SWW)

Zu jedem Kongruenzsatz existiert ein entsprechender **Ähnlichkeitssatz**, wenn man die Übereinstimmung der Seiten durch die Übereinstimmung der entsprechenden Seitenverhältnisse ersetzt, wobei bei dem letzten Satz (SWW) überhaupt keine besondere Eigenschaft der Seite gefordert wird.

- Scheitelwinkel sind stets gleich

Winkel an Parallelen, welche identisch sind:

- Stufenwinkel
- Wechselwinkel

**Satz 2 (Innenwinkelsatz für Dreiecke).** Die Innenwinkelsumme im Dreieck beträgt stets  $180^\circ$ .

Ein Beweis ist dadurch möglich, dass man die Parallele zu einer Seite durch den gegenüberliegenden Eckpunkt einzeichnet und Winkelsätze an Parallelen anwendet.

**Satz 3 (Innenwinkelsatz für n-Ecke).** Die Innenwinkelsumme im n-Eck beträgt stets  $180^\circ \cdot (n - 2)$ .

Eine Unterteilung in Dreiecke und ein Abzählen der Dreiecke führt mit dem Innenwinkelsatz für Dreiecke zum Beweis.

**Definition 3 (Kreis).** Ein Kreis ist eine Menge von Punkten, welche von einem Punkt, dem Mittelpunkt, einen konstanten Abstand, den Radius, haben.

**Satz 4 (Zentri-Peripheriewinkelsatz).** *Peripheriewinkel sind stets doppelt so groß wie ihre Zentriwinkel.*

Diesen Satz kann man mit den Eigenschaften des Kreises, gleichen Basiswinkeln im gleichschenkligen Dreieck und dem Innenwinkelsatz im Dreieck beweisen.

## 2 Zirkel 09.09.2009

Thema: Lösen geometrischer Aufgaben - Wiederholung grundlegender Sätze, Vorgehensweise und Beweisschritte bei geometrischen Beweisen, Anwendung an Aufgaben

- Wiederholung geometrischer Sätze

Wiederholung: Begriffe am Kreis:

Mittelpunkt, Radius, Durchmesser, Passante, Tangente, Sekante, Sehne

**Satz 5 (Sehnenvierecke).** Das Viereck ABCD ist ein Sehnenviereck.

$\Leftrightarrow$  Im Viereck ABCD gilt  $\angle ADB = \angle ACB$ .

(entspricht Peripheriewinkelsatz über  $\widehat{AB}$ )

$\Leftrightarrow$  Im Viereck ABCD gilt  $\angle BAC = \angle BDC$ .

(entspricht Peripheriewinkelsatz über  $\widehat{BC}$ )

$\Leftrightarrow$  Im Viereck ABCD gilt  $\angle CBD = \angle CAD$ .

(entspricht Peripheriewinkelsatz über  $\widehat{CD}$ )

$\Leftrightarrow$  Im Viereck ABCD gilt  $\angle DCA = \angle DBA$ .

(entspricht Peripheriewinkelsatz über  $\widehat{DA}$ )

$\Leftrightarrow$  Im Viereck ABCD gilt  $\angle DAB + \angle BCD = 180^\circ$ .

(entspricht Summe gegenüberliegender Winkel im Sehnenviereck ist  $180^\circ$  - hier bei A und C)

$\Leftrightarrow$  Im Viereck ABCD gilt  $\angle CBA + \angle CDA = 180^\circ$ .

(entspricht Summe gegenüberliegender Winkel im Sehnenviereck ist  $180^\circ$  - hier bei B und D)

Dieser Satz über Sehnenvierecke ermöglicht also, dass man aus **einer** Aussage über zwei Winkel sofort **fünf** andere Winkelbeziehungen erhält! Beachte, dass dies Äquivalenzaussagen sind, das bedeutet auch, dass, wenn man zwei gleiche oder sich zu  $180^\circ$  ergänzende Winkel besitzt und man ihre Schenkel entsprechend schneiden kann, so erhält man **immer** ein Sehnenviereck!

Wiederholung: Kongruenzsätze als Äquivalenzaussage - man kann aus der Gleichheit von gewissen **drei** Größen im Dreieck folgern, dass **alle** restlichen Größen gleich sind.

## Lösen von Geometrieaufgaben

Vor dem Beginn des Lösens einer Geometrieaufgabe ist stets eine **geeignete Skizze** anzufertigen, welche möglichst keinen besonderen Spezialfall darstellt.

Aufgabe: Zeige:  $A \Rightarrow B!$

Vorgehensweisen:

- *Vorwärtsarbeiten:* man beginnt bei der Voraussetzung A und versucht aus dieser zu schließen.

- *Rückwärtsarbeiten*: man beginnt bei der Behauptung und schaut sich an, wie man diese nachweisen kann.
- *Annahme der Voraussetzung und der Behauptung*: wenn die Aussage  $A \Rightarrow B$  wahr ist, dann führt die Annahme von Voraussetzung und Behauptung zu den gleichen geometrischen Figuren, wie wenn man nur die Voraussetzung voraussetzt.  
Dies ermöglicht das **Erkennen von Zwischenschritten** im Beweis (Sehnenvierecke, kongruente/ähnliche Dreiecke...)
- *Konstruierbarkeit betrachten* - Wie würde ich diese Figur konstruieren? - Existiert eine äquivalente, einfachere Aufgabenstellung?  $\Rightarrow$  man erkennt, wo das Problem seine Schwierigkeiten besitzt; eventuell kann man unnötige Punkte aus der Aufgabenstellung entfernen
- *Was bedeutet die Aufgabenstellung?*  $\Rightarrow$  Wie gehe ich bei bestimmten Aufgabenstellungen vor?, Welche Aussagen kann ich am einfachsten zeigen?  
(z.B. man soll zeigen, dass sich drei Geraden schneiden: häufig günstig: man schneide 2 Geraden und zeige, dass die dritte Gerade dadurch geht, häufig ungünstig: man schneidet die Geraden in verschiedenen Punkten und führt dies zum Widerspruch;  
oder man soll zeigen, dass zwei Geraden zueinander parallel sind: meist günstig: man zeigt, dass zwei Wechselwinkel gleich sind, meist ungünstig: man nimmt an es gibt einen Schnittpunkt und führt dies zum Widerspruch)  
 $\Rightarrow$  die Aufgabenstellung in eine **geeignete** mathematische Beziehung übersetzen
- *Plausibilität prüfen* - Betrachten von Spezial-/Extremfällen (z.B. Quadrat statt Viereck betrachten, Dreiecke mit zwei Winkeln von fast  $90^\circ$  betrachten) $\Rightarrow$  Überprüfung ob Zwischenschritte im Beweis stimmen könnten (wenn es im Spezialfall/Extremfall nicht gilt, so gilt es auch im allgemeinen Fall nicht)
- ...

Die oben genannten Vorgehensweisen stellen eine möglichst große **Auswahl an Strategien** bei dem Lösen von Geometriaufgaben dar. Häufig ist es sinnvoll sie **kombiniert** und abwechselnd anzuwenden um die Aufgabe zu lösen.

Wichtig ist es vor allem die Aussagen in eine möglichst **einfache mathematische Form** zu bringen, die ich gut verwenden kann (siehe Text unter Beweisschritte), **jede Voraussetzung** zu nutzen und bei jeder **neuer Erkenntnis** sofort zu erkennen ob diese (eventuell mit einer anderen Aussage) zu einer weiteren neuen Erkenntnis führt.

Um Geometriaufgaben lösen zu können, muss man die grundlegenden Sätze kennen. Man sollte so vorgehen, dass man **jede Aussage** (egal ob sie aus der Voraussetzung, Behauptung oder aus einem Zwischenschritt ist) **in möglichst viele andere Aussagen umzuwandeln**, welche aus dieser folgen und dann diese so zu **filtern**, dass man durch geeignete Kombination den Beweis erhält. Dies ist vor allem Übungssache.

häufige Beweisschritte:

- Ähnlichkeit/Kongruenz von Dreiecken
- gleichschenklige/ gleichseitige Dreiecke
- Sätze am Kreis, Sehnenvierecke
- Erzeugung/Zerstörung von Symmetrien durch Bewegungen
- Winkel an Parallelen
- Innenwinkelsatz
- Ecktransversalen im Dreieck (Seitenhalbierenden, Winkelhalbierenden, Höhen)

- Betrachtung von Flächeninhalten
- Strahlensätze
- ...

Vergewissere dich, welche Beziehungen die oben genannten Beweisschritte darstellen. Sind die Beziehungen **Winkel- oder Längenbeziehungen** oder beides? Häufig sind Geometrieaufgaben vorrangig von Winkeln oder vorrangig von Längenverhältnissen geprägt. Deswegen sollte man sich überlegen, ob gewisse Sätze in dem Beweis hilfreich sein könnten. Häufig ist es wichtig die Aussagen der Voraussetzung auf eine **einheitliche Form** zu bringen, das heißt man wandelt alle Aussagen in Winkelaussagen oder alle Aussagen in Seitenaussagen um.

Aufgabe [440833](#), [460936](#)

### 3 Zirkel 23.09.2009

Thema: Weitere Sätze am Kreis

Einführungsaufgabe:

Man überführe die erste Konstellation der Münzen in die beiden anderen, wobei man bei jeder Verschiebung einer Münze, keine andere Münze verschieben darf und nach jeder Verschiebung die Münze an genau zwei andere Münzen grenzen muss.



**Satz 6 (Sehntangentenwinkelsatz).** *Der Sehntangentenwinkel ist stets so groß wie der Peripheriewinkel über der zugehörigen Sehne.*

Zum Beweis nutze man die Eigenschaft der Tangente, dass sie senkrecht zum Berührungsradius steht, sowie die übliche Herangehensweise, dass man gleichschenklige Dreiecke mit dem Radius als Schenkel im Kreis erhält. Dies führt mit Innenwinkelsatz und Zentriperipheriewinkelsatz zum Ziel.

**Satz 7 (Sehnensatz).** *Schneiden sich zwei Sehnen  $\overline{AB}$  und  $\overline{CD}$  im Punkt  $P$ , so gilt:  $\overline{AP} \cdot \overline{PB} = \overline{CP} \cdot \overline{PD}$ , das heißt, das Produkt der Sehnenabschnitte zu einem Punkt  $P$  ist stets konstant.*

**Satz 8 (Sekantensatz).** *Schneiden sich zwei Sekanten  $\overline{AB}$  und  $\overline{CD}$  im Punkt  $P$  (hier außerhalb des Kreises), so gilt:  $\overline{AP} \cdot \overline{PB} = \overline{CP} \cdot \overline{PD}$ , das heißt, das Produkt der Sekantenabschnitte zu einem Punkt  $P$  ist stets konstant.*

**Satz 9 (Sekantentangentensatz).** *Schneidet eine Sekante  $\overline{AB}$  die Tangente des Kreises am Punkt  $T$  im Punkt  $P$ , so gilt:  $\overline{AP} \cdot \overline{PB} = \overline{TP}^2$ .*

Aus diesen drei Sätzen folgt, dass das Produkt der Streckenlängen von einem Punkt  $P$  zu den Schnittpunkten einer Gerade, durch diesen Punkt, mit dem Kreis lediglich von dem Abstand von  $P$  zum Mittelpunkt des Kreises abhängt. Ein Beweis dieser Sätze ist über das Erkennen zweier ähnlicher Dreiecke möglich und das Aufstellen der entsprechenden Seitenverhältnisse.

Aufgabe [460936](#)

## 4 Zirkel 30.09.2009

Thema: Vollständige Induktion

Einführungsaufgabe:

Man zeige, dass die Mittelsenkrechte einer Sehne AB durch den Mittelpunkt M des zugehörigen Kreises geht.

Idee:  $\triangle ABM$  ist gleichschenkelig. Nun zeige man, dass Höhe und Mittelsenkrechte der Basis identisch sind (durch kongruente Dreiecke).

### Vollständige Induktion

Wenn man eine zu beweisende Aussage  $A(n)$  (in Abhängigkeit von einer natürlichen Zahl  $n \in \mathbb{N}$  gegeben hat), so bietet es sich häufig an die Aussage per vollständiger Induktion zu beweisen.

Prinzip der vollständigen Induktion:

- man zeigt  $A(1)$
- man zeigt, dass aus  $A(n)$  für alle  $n \in \mathbb{N}$  die Aussage  $A(n+1)$  folgt

Dadurch wäre die Aussage dann für alle natürlichen Zahlen  $n$  gezeigt.

Ausführlich gliedert sich der Beweis in verschiedene Teile, welche im Folgenden am Beispiel der Summenformel der ersten  $n$  natürlichen Zahlen dargestellt werden:

Behauptung:  $1 + 2 + 3 + 4 + \dots + (n-1) + n = \frac{n \cdot (n+1)}{2}$

Beweis durch vollständige Induktion:

Induktionsanfang:  $n = 1$

linke Seite: 1

rechte Seite:  $\frac{1 \cdot (1+1)}{2} = 1$

Es ergibt sich eine wahre Aussage.

(Man setzt in die Behauptung  $n=1$  ein und zeigt die Aussage dafür. Dies ist der erste Teil des Prinzips der vollständigen Induktion.)

Induktionsvoraussetzung:

$1 + 2 + 3 + 4 + \dots + (n-1) + n = \frac{n \cdot (n+1)}{2}$

(Die Aussage  $A(n) \Rightarrow A(n+1)$  ist zu zeigen. Es reicht dies unter der Voraussetzung, dass  $A(n)$  wahr ist, zu zeigen, da für falsche  $A(n)$  die Aussage ( $A(n) \Rightarrow A(n+1)$ ) immer wahr ist.)

Induktionsbehauptung:

$1 + 2 + 3 + 4 + \dots + (n-1) + n + (n+1) = \frac{(n+1) \cdot (n+2)}{2}$

(Die entsprechende Behauptung zur Induktionsvoraussetzung.)

Induktionsschritt:  $n \rightarrow n+1$

Es gilt die Induktionsvoraussetzung:

$1 + 2 + 3 + 4 + \dots + (n-1) + n = \frac{n \cdot (n+1)}{2}$

Man addiere nun auf beiden Seiten der Gleichung  $n + 1$ .

$$1 + 2 + 3 + 4 + \dots + (n - 1) + n + (n + 1) = \frac{n \cdot (n + 1)}{2} + (n + 1)$$

Durch Umformen der rechten Seite folgt:

$$1 + 2 + 3 + 4 + \dots + (n - 1) + n + (n + 1) = \frac{n \cdot (n + 1)}{2} + (n + 1) = \frac{n \cdot (n + 1) + 2(n + 1)}{2} = \frac{(n + 1) \cdot (n + 2)}{2}$$

Es ergibt sich demnach die Induktionsbehauptung.

(Der Induktionsschritt entspricht dem Beweis von  $(A(n) \Rightarrow A(n + 1))$ .)

q.e.d.

Bei Gleichheitsaussagen (oder Ungleichungen) mit Summen oder Produkten geht der Induktionsschritt darin über, zu zeigen, dass  $L(n + 1) - L(n) = R(n + 1) - R(n)$  bzw.  $\frac{L(n+1)}{L(n)} = \frac{R(n+1)}{R(n)}$  ist, wobei  $L(n)$  und  $R(n)$  jeweils die linke bzw. rechte Seite der Gleichung sind.

Dies kann man dadurch im Beweis umsetzen, dass man im Induktionsschritt zu der Induktionsvoraussetzung das jeweilige nächste Glied der Summe addiert bzw. das nächste Glied des Produkts multipliziert und die andere Seite solange umformt, bis man die Induktionsbehauptung erhält. Dabei empfiehlt es sich durchaus auch rückwärts zu arbeiten.

Lösen der Aufgaben 1.(a)-(d), 2. (a), (h), 3.(a) und 4.(a) der Aufgabensammlung von Jelena Djokić für vollständige Induktion auf der LSGM-Seite.

## 5 Olympiadevorbereitung

Olympiadaufgaben sollten immer so gestaltet sein, dass sie mit den Mitteln, welche die Schüler besitzen, lösbar sind. Dieses zusätzliche Wissen kann man manchmal auch bei den Aufgaben anwenden. Im folgende Teil wiederhole ich themenweise verschiedene Vorgehensweisen oder auch Sätze und gebe Aufgabenbeispiele aus den letzten Jahren dazu, welche ihr unter <http://www.mathematik-olympiaden.de/archiv.html> nachlesen könnt.

### Zahlentheorie

#### Modulorechnung

*Kurze Einführung in die Modulorechnung:*

Modulorechnung ist das Rechnen mit Resten ganzer Zahlen bezüglich einer ganzen Zahl größer oder gleich 2, welche Modul genannt wird. Man ordnet dazu alle ganzen Zahlen, welche den gleichen Rest  $r$  bezüglich dem Modul  $m$  lassen in eine Restklasse  $[r]_m$  ein. Man schreibt  $a \equiv b$  modulo  $m$  (gelesen:  $a$  kongruent  $b$  modulo  $m$ ), wenn  $a$  und  $b$  den gleichen Rest bezüglich  $m$  haben.

Formal gelten also folgende Äquivalenzaussagen für alle  $a, b, m \in \mathbb{Z}, m \geq 2$ :

Es existieren ganze Zahlen  $a', b'$  und  $r$  mit  $0 \leq r < m, a = a' \cdot m + r$  und  $b = b' \cdot m + r$

$\Leftrightarrow$  Es existiert ein  $k \in \mathbb{Z}$  mit  $a - b = k \cdot m$

$\Leftrightarrow a \equiv b$  modulo  $m$

$\Leftrightarrow$  Es existiert ein  $r \in \mathbb{Z}$  mit  $a \in [r]_m$  und  $b \in [r]_m$

Schreibe jeweils 10 Zahlen aus folgenden Restklassen auf:  $[3]_4, [7]_3, [-24]_5, [12]_6, [0]_2$

Restklassen sind Mengen. Diese sind gleich, wenn sie genau die gleichen Elemente enthalten.

Wie viele verschiedene Restklassen gibt es bezüglich einem Modul  $m$ ?

Es gelten folgende *Rechenregeln*:

Wenn  $a \equiv b$  modulo  $m$ ,  $c \equiv d$  modulo  $m$  und  $k \in \mathbb{Z}$ , so gilt auch:

$$a \equiv b + k \cdot m \text{ modulo } m$$

$$a + c \equiv b + d \text{ modulo } m$$

$$a \cdot c \equiv b \cdot d \text{ modulo } m$$

Wenn  $k > 0$ :  $a^k \equiv b^k$  modulo  $m$

Weise diese Aussagen nach!

(Zusatz: Lässt sich eine entsprechende Aussage für die Division finden?)

Es gilt für jeden Modul  $m$ : Wenn  $a = b$ , so ist auch  $a \equiv b$  modulo  $m$ .

Beachte, dass du für  $a$  und  $b$  beliebige Terme ganzer Zahlen einsetzen kannst! Dies erleichtert bei geeigneter Wahl des Moduls das Lösen von Gleichungen ganzer Zahlen erheblich!

Betrachte nochmal die letzte Rechenregel. Welche Zahlen  $a$  muss ich untersuchen um alle Reste von  $a^k$  für ein festes  $k$  zu berechnen? (betrachte  $k$  gerade und  $k$  ungerade einzeln)

Berechne alle quadratischen Reste (also  $k=2$ ) modulo 3 und modulo 4! Was sagt dies darüber aus ob eine Zahl Quadratzahl sein kann oder nicht?

Nun betrachten wir  $a^k$  bei konstantem  $a$  und veränderbarem  $k$ . Zeige, dass  $a^k$  periodisch wird! (Tipp: Rekursion)

Berechne  $7^{2839}$ ,  $7^{2840}$ ,  $7^{2841}$  und  $7^{2842}$  modulo 5 sowie  $3^{1232} \cdot 4^{923} - 32^{4876}$  modulo 7.

Beispiele: 390921 (lineare diophantische Gleichung) 380922 (Reste von Potenzen) 421022 (ggT-Reste von Kuben)

Leite die Teilbarkeitsregeln für die Zahlen 2, 3, 5, 9, 10 und 11 her, indem du die Dezimaldarstellung einer Zahl ausgeschrieben mit ihren Zehnerpotenzen modulo der Zahl nimmst, zu der du die Teilbarkeitsregeln finden willst (du ersetzt also alle Zehnerpotenzen durch ihren Rest modulo dieser Zahl und interpretierst das Ergebnis).

### Teilbarkeitsregel 9

Beispiele: 411023 440924 441024 470921

### Teilbarkeitsregel 11

Beispiel: 391021

### Primfaktorzerlegung

Bei Zahlentheorieaufgaben bietet sich häufig eine Primfaktorzerlegung an.

Bestimme die Primfaktorzerlegung von 1001 und 2009.

Beispiel: 431022

### Anzahl der Teiler von Zahlen bestimmen

Es gibt einige Aufgaben bei denen man einfach nur die Anzahl der Teiler von Zahlen bestimmen muss. Dazu hilft folgender Satz:

**Satz 10 (Anzahl der Teiler einer natürlichen Zahl größer 1).** Sei  $a = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \dots \cdot p_n^{a_n}$  die Primfaktorzerlegung von  $a$  mit paarweise verschiedenen Primzahlen  $p_1, \dots, p_n$  und positiven ganzen Zahlen  $a_1, \dots, a_n$ . Dann ist die Anzahl der Teiler (inklusive der unechten Teiler 1 und  $a$  selbst) von  $a$  genau  $(a_1 + 1) \cdot (a_2 + 1) \cdot (a_3 + 1) \cdot \dots \cdot (a_n + 1)$ .



(Wie viele Teiler haben die Zahlen 15, 24, 64, 78, 81? Prüfe dies mit der Formel und durch Aufschreiben aller Teiler! Wie heißt die kleinste positive ganze Zahl mit genau 11 bzw. genau 12 Teilern? Beweise den Satz über die Teileranzahl!)

Beispiele: 381021 400921

### Primzahlaufgabe

Bei diesen Aufgaben geht es darum zu zeigen, dass bestimmte Terme von Primzahlen durch andere Zahlen teilbar sind. Man sollte versuchen diesen Term möglichst weit zu faktorisieren (als Produkt schreiben) und dann die Teilbarkeit der einzelnen maximalen Primzahlpotenzen zu zeigen (also z.B. bei  $24 = 2^3 \cdot 3$  zeigt man Teilbarkeit durch die 2-erpotenz 8 und durch 3). Man nutzt dabei aus, dass wenn eine Zahl durch 2 andere teilerfremde Zahlen teilbar ist, so ist sie auch durch deren Produkt teilbar.

Beispiel: 420922 (dritte binomische Formel)

### Bastelaufgaben

Bei solchen Aufgaben, ich habe sie hier Bastelaufgaben genannt, geht es darum aus bestimmten Voraussetzungen bestimmte Zahlen zu finden. Dabei sollte man versuchen Wissen aus den anderen Kategorien wie aus der Modulorechnung oder Teilbarkeitsaussagen anzuwenden um möglichst schnell zum Ziel zu kommen. Man sollte die Aufgabe solange vereinfachen bis die vollständige Fallunterscheidung nicht mehr aufwendig ist.

Beispiele: 400923 410924 (Teilbarkeitsregel 4) 450923 471023 (Teilbarkeitsregel 3)

### Ungleichungen

Hier ist insbesondere auch das Wissen anwendbar, dass die Ungleichung für dich lösbar ist und die Lösungsmenge nicht zu schwierig darstellbar sein darf. Daraus folgt meistens, dass in der Lösungsmenge nur der Gleichheitsfall ist oder die Ungleichung für alle Zahlen gilt.

1.Tipp: Häufig hilft ein Umformen in Quadrate. Das bedeutet man versucht die Ungleichung so umzuschreiben, dass auf einer Seite die Summe von Quadraten (und/oder anderen nicht-negativen Zahlen steht) und auf der anderen Seite 0. Dann hat man die Ungleichung gelöst, da Quadrate reeller Zahlen stets nicht-negativ sind und damit diese Seite immer größer oder gleich 0 ist. Man erhält die richtigen Quadrate am einfachsten durch quadratische Ergänzung. (Wiederhole: binomische Formeln)

Diese Methode ist sehr häufig anwendbar. Insbesondere wenn nur Terme wie  $a^2, b^2, a, b, ab$  und 1 und Vielfache davon vorkommen, eignet sich diese Vorgehensweise.

Beispiel: 480923, 481015

2.Tipp: Mittelungleichung anwenden

Es gilt für alle positiven reellen Zahlen a und b:

$$\sqrt{\frac{a^2 + b^2}{2}} \geq \frac{a + b}{2} \geq \sqrt{ab} \geq \frac{2}{\frac{1}{a} + \frac{1}{b}}$$

Gleichheit gilt genau für  $a=b$ . (Übung: Beweise diese Ungleichung durch Umformen in Quadrate auf einer Seite und sodass auf der anderen Seite 0 steht. Vergewissere dich, dass eventuelles Qua-

drieren erlaubt ist)

(Zusatz: Man kann diese Ungleichung auch noch verallgemeinern zu: Es gilt für alle positiven reellen Zahlen  $a_1, a_2, \dots, a_n$ :

$$\sqrt{\frac{a_1^2 + a_2^2 + \dots + a_n^2}{n}} \geq \frac{a_1 + a_2 + \dots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \dots a_n} \geq \frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_n}}$$

Gleichheit gilt genau bei  $a_1 = a_2 = \dots = a_n$ .)

Die Mittelungleichung ist ebenfalls eine Standardvorgehensweise. Man sollte prüfen ob sie anwendbar ist. (eher in höheren MO-Stufen)

3.Tipp: Weiterhin ist häufig nützlich: Für positive reelle Zahlen  $a, b$  und  $x$  gilt stets:

$$\frac{a}{b} + \frac{b}{a} \geq 2$$

bzw.

$$x + \frac{1}{x} \geq 2$$

(Übung: Beweise diese Ungleichung durch Umformen in Quadrate, sodass auf einer Seite das Quadrat einer reellen Zahl steht und auf der anderen Seite 0. Wann gilt Gleichheit? Was passiert bei negativen Zahlen?)

Beispiel: 450922 (man beachte auch was bei negativen Zahlen passiert - beachte, dass sich das Vorzeichen bei Multiplikation mit negativen Vorzeichen umdreht; kann man auch ohne Fallunterscheidung beim Umformen die Aufgabe lösen?)

4.Tipp: Dreiecksungleichung

Bei Geometrieaufgaben, bei denen Ungleichungen zu beweisen sind und sonst nicht viel über das geometrische Objekt bekannt ist, hilft meistens nur die Dreiecksungleichung. Man suche sich also möglichst viele Dreiecke und stelle die Dreiecksungleichungen auf und addiere diese dann so, dass man die zu beweisende Aussage erhält.

Beispiel: 390924

5.Tipp: Ungleichungen getarnt als Gleichungen:

Wenn man mehr reelle Variablen (bei ganzen Zahlen hilft es nicht) als Gleichungen hat, so ist die Gleichung (das Gleichungssystem) meistens der Gleichheitsfall einer Ungleichung (ansonsten wäre die Aufgabe für Matheolympiaden zu schwer). Dann wird die Aufgabe meistens ziemlich einfach und die anderen Tipps sind anwendbar.

Beispiel: 391022

6.Tipp: vollständige Induktion:

Dies eignet sich wie immer nur bei Aussagen mit natürlichen Zahlen. Doch dann ist es praktisch immer hilfreich. Die Vorgehensweise ist wie im letzten Zirkel behandelt.

Beispiel: 390922

### 7.Tipp: geeignetes Abschätzen:

Wenn man Aussagen mit Produkten oder Summen hat, ist ein geeignetes Abschätzen sinnvoll. Man kann versuchen die einander gegenüberliegenden (größte und niedrigste, zweitgrößte und zweitkleinste usw.) Zahlen paarweise gegen einen entsprechenden Term von der anderen Seite abzuschätzen.

(Zusatz: Auch das Teleskopprinzip ist häufig sinnvoll. Man zerlegt aufeinanderfolgende Terme in Einzelterme, welche sich gegenseitig aufheben. Also z.B.  $\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$  ist hilfreich wenn man die Summe  $\frac{1}{1(1+1)} + \frac{1}{2(2+1)} + \dots + \frac{1}{n(n+1)}$  berechnen will.)

Beispiel: 401023 (benutze die dritte binomische Formel und Tipp 1)  
(391042)

(Zusatz: 8.Tipp: Umordnungsungleichung:

Jeder kennt das Prinzip: Man darf 1, 2, 4 beziehungsweise 6 Geldstücke aus 4 Töpfen nehmen in dem sich Ein-Cent-, Zwei-Cent-, Fünf-Cent- und Zehn-Cent-Stücke befinden. Wann bekommt man am meisten Geld? Wann am wenigsten?

Formal beschreibt dies die Umordnungsungleichung:

**Satz 11 (Umordnungsungleichung).** Sei  $n$  eine natürliche Zahl und zwei Folgen reeller Zahlen  $[a_n]$  und  $[b_n]$  mit  $0 \leq a_1 \leq a_2 \leq \dots \leq a_n$  sowie  $0 \leq b_1 \leq b_2 \leq \dots \leq b_n$  gegeben. So ist die Summe der Produkte, von Zahlen einer Folge mit Zahlen der anderen Folge, wobei jede Zahl genau einmal verwendet wird, maximal, wenn Glieder mit gleichen Indizes miteinander multipliziert werden und minimal, wenn Glieder mit entgegengesetzten Indizes multipliziert werden.

)

## Kombinatorik (hier lediglich Abzählaufgaben)

Man sollte auch hier versuchen das Problem solange zu vereinfachen, bis eine Fallunterscheidung machbar ist. Schreibe die Aussage zunächst abstrakt. Nutze Symmetrien aus. Man schaue ob man gegebenenfalls ohne Beschränkung der Allgemeinheit gewisse Dinge annehmen kann (Symmetrien zerstören)?

Wie viele Möglichkeiten gibt es die Zahlen von 1 bis  $n$  anzuordnen?

Beispiele: 380921 410921 420921 421021 430921 471021

## vollständige Induktion

Vollständige Induktion eignet sich nicht nur bei dem Nachweisen von Gleichheiten oder Ungleichungen. Immer wenn Aussagen mit natürlichen Aussagen im Zusammenhang stehen, kann man vollständige Induktion versuchen. Man erkennt bei einigen Aufgaben manchmal intuitiv wie man von der Aussage für  $n$  Objekte auf  $n+1$  Objekte kommt. Dann ist Induktion genau richtig. (typische Aufgabentypen: Parkettierungen von Flächen, Folgenaufgaben, Färbeaufgabe)

Beispiele: 430922b (geht es auch mit 2 Farben?) 470924c 471022b

## Textaufgaben

Benenne geeignete Größen durch Variablen und schreibe die Aussagen des Textes in Gleichungen und Ungleichungen um. Lege die den Definitionsbereich geeignet fest. Löse danach das System der Aussagen.

Beispiele: 380924 430923 460921 470923 480922

## Schubfachprinzip

Wenn man  $n \cdot k + 1$  Elemente auf  $n$  Schubfächer verteilt, so existiert mindestens ein Schubfach mit  $k+1$  Elementen.

Man muss nun versuchen Schubfächer und Elemente geeignet zu wählen, dass diese Aussage der Behauptung entspricht.

Beispiel: 461022

## Wahrscheinlichkeitsrechnung

Es gilt: Wenn Ergebnisse die gleiche Wahrscheinlichkeit haben, so ist die Wahrscheinlichkeit, dass ein Ereignis eintritt gleich der Anzahl der Ergebnisse im Ereignis durch die gesamte Anzahl der Ergebnisse.

(z.B. beim Würfeln: die Wahrscheinlichkeit eine 2 oder 5 zu würfeln ist  $\frac{2}{6}$  ( $= \frac{1}{3}$ ), da jede Zahl mit der gleichen Wahrscheinlichkeit auftaucht)

Beispiel: 381022

(Zusatz:

## Spieltheorie

Bei Spieltheorieaufgaben läuft es meistens auf folgendes (hier abstrakt beschriebenes) Prinzip hinaus:

Man hat zwei Klassen A und B von Spielpositionen. Von A kommt man durch einen Spielzug immer zu einer Spielposition von B. Von B kommt man durch keinen Spielzug zu einer anderen Spielposition in B.

Die Taktik ist dann folgendermaßen: Spieler A beginne in der Spielpositionsklasse A. Er kann nach Definition immer nach B ziehen. Spieler B muss jedoch dann wieder in Spielpositionsklasse A ziehen, wenn er dran ist. Somit kann Spieler A den Spieler B immer dazu zwingen von der Spielklasse B aus zu ziehen. In dieser liegt dann auch die Endposition aus der kein Zug mehr möglich ist und Spieler B hat verloren.

Man muss also versuchen geeignete Spielpositionsklassen zu wählen, welche diese Eigenschaften erfüllen. Dies geht am Besten, wenn man kleine Zahlenbeispiele wählt und diese untersucht und dann eine Vermutung aufstellt. In der Matheolympiade muss nur der Lösungsweg aber nicht die Lösungsfindung ersichtlich sein! Ihr könnt also bei der Reinschrift von den beiden Spielpositionsklassen ausgehen und ihre Eigenschaften nachweisen. Zeigt auch, dass das Spiel irgendwann terminieren (=enden/aufhören) muss!

Bei manchen Aufgaben kann man auch Symmetrien ausnutzen. Indem man immer symmetrisch zum Gegenüber spielt, hat der Gegner keine Chance die Symmetrie zu brechen und man kann immer den letzten Zug spielen.

Beispiel: 440922)

### weitere Tipps

- Bei einer Aufgabe mit rationalen Zahlen bietet es sich häufig an die rationale Zahl als Bruch zweier ganzer Zahlen zu schreiben, deren größter gemeinsamer Teiler 1 ist. (z.B. 381024, hier ist auch Zurückführen auf einfachere Probleme sinnvoll)
- benutze ein Prinzip wie indirekter Beweis oder Extremalprinzip z.B. 450921
- wende wo es geht binomische Formeln an, Faktorisierere wenn es möglich ist
- probiere bei kleinen Zahlen das Problem aus

### weitere Aufgaben

Ein wenig rechnen: 440921

Quadratische Gleichung in ganzen Zahlen: 431023

minimale Anzahl finden: 460922

geeignetes Argumentieren bei Selbstbezüglichkeit: 460924

Probieraufgabe: 480921

Polyeder: 400922

## Geometrie

Geometrie haben wir schon in den vorherigen Stunden häufig behandelt.

Wiederholt nochmal Flächenberechnung am Dreieck, am Kreis und am Trapez. Schaut euch nochmal die Sachen an, die wir behandelt haben.

Weitere wichtige Sätze findet man beispielsweise auf <http://www.olympiade-mathematik.de/geometrie.php>

.

Hier sind nun noch die geordneten MO-Aufgaben der letzten Jahre:

Berechnung am Kreis - Flächeninhalte: 380923

gleicher Schnittpunkt: 381023

Gleichlange Strecken, Orthogonalität: 390923

gleichschenkliges Dreieck: 391024

Viereck, Sehnenviereck: 400924

Sehntangentensatz: 401024

Berechnung am Kreis - Längen: 410922

Inkreis, Umkreis bei n-Eck: 411024

Mittellinien Viereck: 420923

Spitzwinkligkeit, Flächenberechnung: 420924

Parallelogramm, Flächenberechnung: 430924

Raumgeometrie: 440923

Flächenberechnung Sechseck: 450924

Flächenberechnung Achteck: 451024

Kreise, spitzwinkliges Dreieck: 460923

Inkreis, Umkreis: 461023

Flächeninhaltsverhältnis: 470922

Parallelogrammformel: 471024

Länge bestimmen, rechter Winkel: 480924

berührende Kreise: 481024

## 6 Zirkel 28.10.2009

Behandlung der Aufgaben der Mathematikolympiade 1.Runde

Beweis, dass  $\sqrt{2}$  irrational ist. (Indirekter Beweis, Darstellung als Quotient zweier ganzer Zahlen, Quadrieren und zum Widerspruch führen)

Summen und Produkte rationaler und irrationaler Zahlen. (Erhält man rationale oder irrationale Zahlen, wenn man rationale/irrationale Zahlen addiert/multipliziert)

## 7 Zirkel 11.11.2009

Thema: Einführung Modulorechnung

**Definition 4 (Rest).** Sei  $z$  eine ganze Zahl und  $m$  eine ganze Zahl größer als 1, so heißt die ganze Zahl  $r$  ( $0 \leq r < m$ ) Rest von  $z$  bei Teilung durch  $m$ , wenn eine ganze Zahl  $k$  existiert mit  $z = k \cdot m + r$ .

**Definition 5 (Restklassen).** Die Restklasse  $[r]_m$  ist die Menge aller ganzen Zahlen  $z$ , welche bei Teilung durch  $m$  den Rest  $r$  lassen. (Dies ist äquivalent dazu, dass  $z - r$  durch  $m$  teilbar ist.)

**Definition 6 (kongruent).** Zwei ganze Zahlen  $a$  und  $b$  heißen genau dann kongruent modulo  $m$  (geschrieben:  $a \equiv b \pmod{m}$ ), wenn sie beide der gleichen Restklasse modulo  $m$  angehören.

**Satz 12.** Es gilt für alle ganzen Zahlen  $a, b, c$  und  $d$ , einen Modul  $m$  und einer natürlichen Zahl  $n$  mit  $a \equiv b \pmod{m}$  und  $c \equiv d \pmod{m}$  stets:

- $a + c \equiv b + d \pmod{m}$
- $a - c \equiv b - d \pmod{m}$
- $a \cdot c \equiv b \cdot d \pmod{m}$
- $a^n \equiv b^n \pmod{m}$

Außerdem gilt auch für alle ganzen Zahlen  $e, f$  und  $g$  und einen Modul  $m$  stets:

Wenn  $e \cdot g \equiv f \cdot g \pmod{m}$ , so gilt auch  $e \equiv f \pmod{\frac{m}{\text{ggT}(m,g)}}$

(wobei wenn  $m$  ein Teiler von  $g$  ist die Aussage unsinnig wird)

Beweis der Divisionsaussage (kurz skizziert)

$g' := \frac{g}{\text{ggT}(m,g)}$  und  $m' := \frac{m}{\text{ggT}(m,g)}$  So entspricht der Behauptung die Aussage: Wenn  $(e - f) \cdot g' \cdot \text{ggT}(m, g) \equiv 0 \pmod{m' \cdot \text{ggT}(m, g)}$ , so gilt auch  $e - f \equiv 0 \pmod{m'}$  oder wenn  $m' \cdot \text{ggT}(m, g)$  ein Teiler von  $(e - f) \cdot g' \cdot \text{ggT}(m, g)$  ist, so ist auch  $m'$  ein Teiler von  $e - f$ . Dies folgt aus der Teilerfremdheit von  $g'$  und  $m'$ .

Berechnung von Resten

Die Modulorechnung ermöglicht die einfache Berechnung von Resten großer Zahlen. Die oberen Rechenregeln ermöglichen dies.

Inbesondere kann man dadurch die letzten  $n$  Ziffern von ganzen Zahlen berechnen, indem man die Zahl modulo  $10^n$  betrachtet.

Beispiel: Letzten beiden Ziffern von  $23465534^{74853462342393}$

Zunächst erkennt man nach der 4.Regel, dass man auch stattdessen die letzten beiden Ziffern von  $34^{74853462342398}$  berechnen kann. Man berechne zunächst Reste kleinerer Potenzen.  $34^1 \equiv$

$34 \bmod 100$ ,  $34^2 \equiv 34 \cdot 34 \equiv 1156 \equiv 56 \equiv -44 \bmod 100$ ,  $34^3 \equiv 56 \cdot 34 \equiv 1904 \equiv 4 \bmod 100$ ,  $34^4 \equiv 4 \cdot 34 \equiv 136 \equiv 36 \bmod 100$ ,  $34^5 \equiv 36 \cdot 34 \equiv 1224 \equiv 24 \bmod 100$ ,  $34^6 \equiv 24 \cdot 34 \equiv 816 \equiv 16 \bmod 100$ ,  $34^7 \equiv 16 \cdot 34 \equiv 544 \equiv 44 \bmod 100$ .

Man hat also nun den Rest 44 erreicht, wobei man den Rest -44 schon vorher erhalten hatte. Da der nächste Rest immer nur von dem vorherigen Rest abhängt (Multiplikation mit 34), kommen danach also wieder die entsprechend negativen Reste vor. Das bedeutet, dass an der Stelle wenn die 44 dran kommen würde, dann die -44 steht. Damit wird der Rest periodisch und zwar hier mit der Periodenlänge 10 und einer Vorperiode der Länge 1.

Der Exponent lässt den Rest 3 bei Teilung durch 10.  $23465534^{74853462342393} \equiv 34^3 \equiv 04 \bmod 100$ . Die Zahl endet auf 04.

Beispiel: Man berechne  $37^{12563426347}$  modulo 11.

37 kann man wieder durch 4 ersetzen. Dann gilt  $4^2 \equiv 16 \equiv 5 \bmod 11$ ,  $4^3 \equiv 20 \equiv 9 \bmod 11$ ,  $4^4 \equiv 36 \equiv 3 \bmod 11$  und  $4^5 \equiv 12 \equiv 1 \bmod 11$ . Wenn ich 1 oder -1 erreicht habe, kann ich einfach die Zahl modulo der Periode betrachten. Hier ist die Periode 5 (da  $4^5$  den Rest 1 lässt, bei -1 müsste man den Exponenten verdoppeln). Damit ist  $37^{12563426347} \equiv 4^2 \equiv 5 \bmod 11$ .

Man überlege sich: Warum erreicht man stets eine Periode, wenn man den Exponenten immer weiter vergrößert? Funktioniert es auch bei der Basis?

Herleitung der Teilbarkeitsregeln am Beispiel der Teilbarkeit durch 9:

Die ausgeschriebene Dezimaldarstellung einer ganzen Zahl  $z$ , laute:

$z = a_0 + 10 \cdot a_1 + 10^2 \cdot a_2 + \dots + 10^{n-1} \cdot a_{n-1} + 10^n \cdot a_n$ , wobei  $a_1, \dots, a_n$  die entsprechenden Ziffern von  $z$  seien. Nun betrachte man diese Zahl  $z$  modulo 9. Wenn man 10 modulo 9 nimmt, so erhält man 1. Entsprechend erhält man auch  $1 \equiv 10 \equiv 10 \cdot 1 \equiv 10 \cdot 10 \equiv 10^2 \equiv 10^2 \cdot 10 \equiv 10^3 \equiv \dots \equiv 10^n \bmod 9$ . Einsetzen in der Darstellung von  $z$  ergibt  $z \equiv a_0 + a_1 + a_2 + \dots + a_{n-1} + a_n \bmod 9$ . Demnach lässt  $z$  den gleichen Rest bei Teilung durch 9 wie die Quersumme von  $z$ . Dadurch kann man die Teilbarkeit von  $z$  durch 9 prüfen, wenn man dies für die Quersumme von  $z$  untersucht.

Lösen der folgenden Aufgabe

Man sucht eine positive ganze Zahl kleiner als 200, mit den Eigenschaften, dass sie bei Teilung durch 3 den Rest 2 lässt, bei Teilung durch 4 den Rest 3, bei Teilung durch 5 den Rest 4 und bei Teilung durch 6 den Rest 5. AuSSerdem ist sie durch 7 teilbar.

Lösungsansatz: Modulo 3, 4, 5 und 6 erhält man laut Aufgabenstellung den Rest -1. Nun kann man zeigen, dass dann auch für das kleinste gemeinsame Vielfache von 3, 4, 5 und 6 diese Zahl diesen Rest lässt und die Umkehrung gilt auch (Zeige dies!). Nun ist nur noch eine entsprechende durch 7 teilbare Zahl in diesem Bereich zu suchen. (Lösung: kgV=60, durch 7 teilbar und Rest -1 mod 60: 119)

## 8 Zirkel 25.11.2009

Thema: Sätze zur Modulorechnung

**Satz 13 (Kleiner Satz von Fermat).** *Es gilt  $a^p \equiv a \bmod p$  für alle Primzahlen  $p$  und ganzen Zahlen  $a$ .*

Wenn  $a$  teilerfremd zu  $p$  ist, so folgt  $a^{p-1} \equiv 1 \bmod p$

**Definition 7 (Phi-Funktion).** Zu einer natürlichen Zahl  $n$  sei  $\varphi(n)$  die Anzahl der natürlichen Zahlen kleiner oder gleich  $n$ , welche zu  $n$  teilerfremd sind.

**Satz 14 (Berechnung von Werten der Phi-Funktion).** Für Primzahlen  $p$  gilt  $\varphi(p) = p - 1$ .  
Für Primzahlpotenzen  $p^k$  gilt  $\varphi(p^k) = p^{k-1} \cdot (p - 1)$ .  
Wenn die Zahlen  $a$  und  $b$  zueinander teilerfremd sind, so gilt  $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ .

**Satz 15 (Satz von Euler).** Es gilt  $a^{\varphi(m)} \equiv 1 \pmod{m}$  für alle ganzen Zahlen  $m > 1$  und alle  $a$  mit  $\text{ggT}(a, m) = 1$ .

Beweis:

Man betrachte die zu  $m$  teilerfremden Zahlen  $a_1, \dots, a_{\varphi(m)}$ , welche kleiner als  $m$  sind. Demnach existiert ein  $a_i$  ( $i \in 1, \dots, \varphi(m)$ ) mit  $a_i \equiv a \pmod{m}$ .

Multipliziert man nun jede der Zahlen  $a_j$  ( $j \in 1, \dots, \varphi(m)$ ) mit  $a$ , so erhält man paarweise verschiedene Zahlen, da wenn zwei Zahlen davon gleich wären, so müsste auch die beiden ursprünglichen Zahlen gleich sein, da man durch  $a$  teilen kann, denn  $\text{ggT}(a, m) = 1$ .

Weiterhin darf auch kein Rest entstehen, welcher einen gemeinsamen Teiler mit  $m$  hat. Demnach bewirkt die Multiplikation mit  $a$  eine Permutation (Vertauschung) der  $a_j$ .

Das bedeutet wegen der Kommutativität der Multiplikation  $a_1 \cdot a_2 \cdot \dots \cdot a_{\varphi(m)} \equiv aa_1 \cdot aa_2 \cdot \dots \cdot aa_{\varphi(m)} \pmod{m}$ .

Da  $a_1 \cdot a_2 \cdot \dots \cdot a_{\varphi(m)}$  teilerfremd zu  $m$  ist, kann man dadurch teilen. Es folgt  $1 \equiv a^{\varphi(m)} \pmod{m}$ .

q.e.d.

Der Satz von Euler ist ein Spezialfall des kleinen Satzes von Fermat.

**Satz 16 (Satz von Wilson).**  $p$  ist genau dann eine Primzahl, wenn  $(p - 1)! \equiv -1 \pmod{p}$ .

Beweis:

Wenn  $p$  keine Primzahl ist, steckt in  $(p - 1)!$  ein Teiler von  $p$ , jedoch ist  $-1$  teilerfremd zu  $p$ .  
Widerspruch

Es ist demnach nur noch zu zeigen, dass wenn  $p$  eine Primzahl ist, dann auch  $(p - 1)! \equiv -1 \pmod{p}$  gilt.

Ähnlich wie bei dem Beweis des Satzes von Fermat erfolgt dieser Beweis.

Diesmal sind die teilerfremden Zahlen zu  $p$  die Zahlen von 1 bis  $p - 1$ . Bildet man alle Paare dieser Zahlen und multipliziert diese miteinander, so kommt (wie nach obiger Begründung im Beweis vom Kleinen Fermat) in jeder Spalte (der Multiplikationstafel) jeder der Reste von 1 bis  $p - 1$  genau einmal vor.

Nun gilt jedoch bei einem Rest  $a$  genau dann  $a^2 \equiv 1 \pmod{p}$ , wenn  $a^2 - 1 \equiv 0 \pmod{p}$  beziehungsweise  $(a - 1) \cdot (a + 1) \equiv 0 \pmod{p}$ , welches bedeutet dass  $a \equiv 1 \pmod{p}$  oder  $a \equiv -1 \pmod{p}$ .

Dies bedeutet, dass es zu jedem Rest zwischen 2 und  $p - 2$  eine andere Zahl daraus gibt, sodass ihr Produkt den Rest 1 lässt.

Demnach gilt  $(p - 1)! \equiv 1 \cdot 1 \cdot \dots \cdot 1 \cdot (p - 1) \pmod{p}$  und damit  $(p - 1)! \equiv -1 \pmod{p}$ .

q.e.d.

Ausblick/ weitere mögliche Anwendungen der Modulorechnung:

Die Periodizität, welche bei Folgen ganzer Zahlen modulo einer Zahl  $m$  meist auftritt, ermöglicht Teilbarkeitsaussagen oder auch Unmöglichkeitssausagen (z.B. keine Zahl lässt den Rest 3 bei Teilung durch 4) für alle ganzen (bzw. natürlichen) Zahlen, durch Betrachtung lediglich endlich vieler Reste.

Man kann Gleichungen der Form  $ax \equiv b \pmod{m}$  lösen, wenn  $b$  durch  $\text{ggT}(a, m)$  teilbar ist indem man  $k \cdot m$  zu  $b$  addiert, sodass es durch  $a$  teilbar ist. Man erhält eine Kongruenzgleichung, wobei  $x$  auf einer Seite allein steht.



## 9 Zirkel 9.12.2009

Thema: Spieltheorie und -praxis

Lösungsstrategien: Symmetrien Ausnutzen, Invarianten finden, Gewinn- und Verlustpositionen bestimmen

### 1. Symmetrien ausnutzen

Ein Spieler spielt immer symmetrisch zu dem vorherigen Zug des anderen Spielers. Dadurch ist er immer in der Lage zu ziehen, solange sich die Züge nicht „überlappen können“ (siehe 3.Aufgabe). Nun ist nur noch zu zeigen, dass das Spiel terminiert, das heißt, dass es nicht unendlich lange dauert. Somit kann der symmetrisch spielende Spieler stets den letzten Zug (welcher existiert, da das Spiel terminiert) machen.

Aufgaben: 411314, 451324, 481313

### 2. Invarianten finden

Invarianten sind feste Größen, etwas das immer gleich bleibt. Häufig läuft die Lösungsstrategie darauf hinaus, dass ein Spieler immer so spielt, dass er den Zug des anderen neutralisiert, sodass also eine bestimmte Größe immer gleich bleibt.

Bsp: 380931

### 3. Gewinn- und Verlustpositionen beginnen

Man beginnt mit kleinen Zahlen und untersucht, wann welcher Spieler gewinnt, bis man eine Regelmäßigkeit festgestellt hat.

Bsp: 481041

Zusatz: Grundy-Werte

Grundy-Werte sind eine weitere Unterteilung der Verlustpositionen. Sie ermöglichen die Zusammenfassung mehrerer Spiele zu einem Spiel.

Jede Position bekommt die kleinste nicht-negative ganze Zahl, welche nicht von dieser Position erreichbar ist (Endpositionen sind damit 0) zugeordnet. Dadurch sind die Gewinnpositionen die Positionen mit Grundy-Wert 0 (Warum?).

Weiterhin erhält man den Grundywert eines Spieles, welches aus mehreren Spielen besteht (sodass man also bei seinem Zug ein Spiel auswählt, in diesem zieht und dann der andere dran ist), indem man die Grundy-Werte der einzelnen Spiele in einer bestimmten Weise addiert. Und zwar stellt man dazu die Zahlen in ihrer Binärdarstellung dar, schreibt sie untereinander und zählt die Einsen in jeder Spalte. Wenn die Anzahl der Einsen ungerade ist, so erhält man wieder eine 1, sonst eine 0.

Überlegt euch, warum man den Grundy-Wert des Gesamtspiels dann erhält! Was bedeutet das wenn es zwei Spiele sind?