

**Korrespondenzzirkel und Schülerseminar
an der Universität Stuttgart**

P.H. Lesky

Fachbereich Mathematik

Institut für

Analysis, Dynamik und Modellierung

Arbeitsmaterial

Kombinatorik

Ein Vertreter soll von Stuttgart nach Reutlingen fahren, danach nach Tübingen, und schließlich wieder nach Stuttgart zurück. Er möchte sich auf der Fahrt ein bisschen die Gegend ansehen und sucht auf der Karte nach interessanten Strassenverbindungen. Er stellt fest, dass ihm 5 Verbindungen von Stuttgart nach Reutlingen zusagen, 2 von Reutlingen nach Tübingen und 4 von Tübingen nach Stuttgart. Wie viele verschiedene Reiserouten kann er daraus zusammenstellen? ...

Dies ist eine Aufgabe aus der Kombinatorik, der Lehre vom Abzählen. Die Kombinatorik gibt Antwort auf Fragen vom Typ „Wie viele Möglichkeiten gibt es ...?“.

Aufgaben

1. Eine frisch gekaufte Gurke wiegt 500g und besteht zu 90% aus Wasser. Nachdem die Gurke ein paar Tage in der Küche gelegen hat, besteht sie nur noch zu 80% aus Wasser. Wie viel wiegt sie jetzt?
Tipp: Berechne zunächst, wieviel die Gurke ohne Wasser wiegen würde.

Aufgaben

2. Ein Stuttgarter Autokennzeichen besteht aus „S“ für Stuttgart, dann zwei oder ein oder kein Buchstaben und dann eine maximal vierstellige Zahl. 0 allein ist als Zahl nicht zugelassen. Wie viele verschiedene solche Kennzeichen gibt es?

Aufgaben

3. Bei einem schwierigen Preisausschreiben sind nur 9 richtige Einsendungen eingegangen. Darunter sollen ein erster, ein zweiter und ein dritter Preis verlost werden. Wie viele verschiedene Möglichkeiten gibt es, diese drei Preise zu verteilen?
Wie viele Möglichkeiten, die Preise zu verteilen, gibt es, wenn die drei Preise gleichwertig sind?

Das Arbeitsmaterial

Serie 1: Mengenlehre (Alle Klassenstufen)

Serie 2: Aussagenlogik (7-8 u. 9-10),
Vollständige Induktion (11-13)

Serie 3: Kombinatorik (7-8),
Vom Dreieck bis zum Vieleck (9-10)
Komplexe Zahlen (11-13)

Serie 4: Ungleichungen in 2 Variablen (7-8),
Zahlentheorie (9-10 u. 11-13)

Das Schülerseminar

Zwei Gruppen: Klasse 8 – 10, Klasse 10 – 13

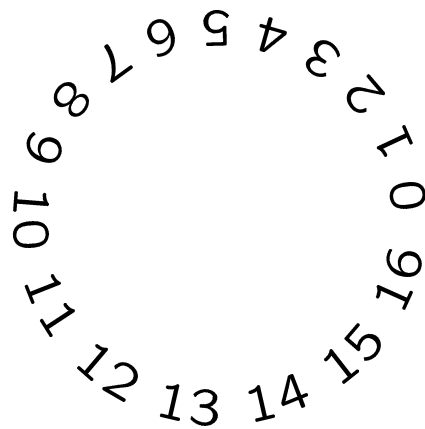
Treffen wöchentlich, 90 Minuten

- Zahlentheorie (Kryptographie)
- Programmieren in C (Euklidischer Algorithmus, Public-key-Verschlüsselung, Erzeugung großer Primzahlen)

Endliche Körper

Die ganzen Zahlen werden durch Restklassenbildung zu einem Kreis aufgerollt:

hier z.B. $\mathbb{Z}/17\mathbb{Z}$



Problem

Alice und Bob wollen geheime Nachrichten austauschen ohne sich zu treffen.

Wie können Sie einen Geheimcode vereinbaren?

Diffie-Hellman Schlüsselaustausch

Alice und Bob vereinbaren öffentlich:
Primzahl p und Primitivwurzel g .

Alice wählt geheim a | Bob wählt geheim b

Alice veröffentlicht: $A = g^a \pmod p$

Bob veröffentlicht $B = g^b \pmod p$

Alice berechnet

$$B^a \pmod p =$$

$$g^{ab} \pmod p = K$$

Bob berechnet

$$A^b \pmod p =$$

$$g^{ab} \pmod p = K$$

Für die Bestimmung von a aus A (diskreter Logarithmus) besteht kein effizienter Algorithmus.

Was bringt's?

- Mathematik macht Spaß
- Klares Denken und Formulieren
- Horizont erweitern, Rolle der Mathematik in Anwendungen
- Erleichterung des Studienbeginns:
Strukturen an Uni kennenlernen
Ansprechpartner an Uni begegnen
- Unterstützung der Lehrer

Seminar

- **Klasse 8 – 9:**
Zu Beginn: 6 Teilnehmer
Stand 2.4.03: 6 Teilnehmer

- **Klasse 10 – 13:**
Zu Beginn: 9 Teilnehmer
Stand 2.4.03: 6 Teilnehmer

Ausblick

- Materialien
- Mitarbeiter
- Finanzierung
- Keplerseminar
- Adresse:
E-Mail:
`zirkel@mathematik.uni-stuttgart.de`
Internet:
`http://www.mathematik.uni-stuttgart.de`
`/studium/schuelerzirkel/`