Elementare Zahlentheorie

Vorlesungsskript

zur Vorlesung Elementare Zahlentheorie gehalten im WS 03/04

an der

Rheinisch-Westfälischen Technischen Hochschule Aachen

von

Prof. Dr. Ulrich Schoenwaelder

Aachen, Mai 2004

Lehrstuhl D für Mathematik
Univ.-Prof. Dr. phil. nat. U. Schoenwaelder
RWTH Aac

Inhaltsverzeichnis

Bemerkung: Man beachte, dass fast immer das Zeichen $\in$ in diesem Dokument durch das Zeichen ? oder das Zeichen $\square$ repräsentiert wird.

§0 Worum geht es?

A. Fachdidaktische Fragen

- Was ist Mathematik?

→ Mathematik ist eine Tätigkeit.

- Welche Tätigkeit?

→ Mathematisches Denken und Handeln.

→ Mathematisches Denken:
- Inhaltliche bzw. semantische Ebenen:
  1. Diskursebene
  2. Diskursebene
  3. Diskursebene
  4. Diskursebene
- Formale bzw. symbolische bzw. syntaktische Ebene:
  5. Diskursebene bzw. Diskursebene S

Es besteht eine enge Beziehung zwischen den Diskursebenen 2 bis 4 und der symbolischen Diskursebene, wir wechseln ständig zwischen diesen. Insbesondere kann ein elektronischer Rechner nur auf der symbolischen Ebene arbeiten, ohne dass er hierbei die Bedeutung (die Semantik) der mathematischen Symbole versteht.

- Wozu unterrichten wir Mathematik? (Ziele des Mathematikunterrichts)

→ Mathematisches Denken und Handeln (Tätigkeiten) kennen lernen und erlernen.

B. Stoff:

In der elementaren Zahlentheorie studieren wir Eigenschaften der Mengen **N**, **Z** und **Q**. Im Vordergrund stehen hierbei insbesondere die ganzen Zahlen. Dazu wollen wir zunächst der Frage nachgehen, was ganze Zahlen eigentlich sind.

Bei der Betrachtung der ganzen Zahlen ist es zunächst notwendig, dass wir wissen und verstehen, was natürliche Zahlen sind. Im Folgenden betrachten wir also die Menge **N** der natürlichen Zahlen. (Wir werden bei der nachfolgenden Konstruktion der natürlichen Zahlen nicht zu sehr ins Detail gehen, da es hierzu eine separate Vorlesung gibt.)

1. Diskursebene:
Auf der ersten Diskursebene betrachten wir konkrete physikalische Objekte. Ein Kind lernt an solchen bereits in der Vorschule das Zählen. Dazu lernt es die Zahlen auswendig (wie einen Reim: eins, zwei, drei, vier, ...) und geht dann, indem es den Reim aufsagt, von einem Objekt zum nächsten.

Im nächsten Schritt lernt es in der Grundschule das Rechnen, ebenfalls an Hand von solchen konkreten physikalischen Objekten.

ein Apfel		ein Apfel		ein Apfel	fünf Apfel
zwei Äpfel	+	zwei Äpfel	=	zwei Äpfel	sechs Äpfel
drei Äpfel		drei Äpfel		drei Äpfel	sieben Äpfel
vier Äpfel				vier Äpfel	
vier Äpfel	+	drei Äpfel	=	sieben Äpfel	

Dazu legt es diese Objekte nebeneinander und zählt die Gesamtzahl ab.

2. Diskursebene:
Nun erfolgt auf der zweiten Diskursebene eine Abstraktion bzw. Idealisierung der physikalischen Ebene aus der 1. Diskursebene. An Stelle mit der Anzahl konkreter Gegenstände zu rechnen, verfährt es jetzt lediglich noch mit den Zahlen. Es erfolgt ein Übergang von den konkreten physikalischen Objekten zur Menge N der natürlichen Zahlen. Dies ist ein wichtiger Lernprozess eines Kindes, welcher erst einmal bewältigt werden muss. Denn woher weiß das Kind, dass zum Beispiel

$$4 + 3 = 7$$

ist? Hierbei geht es in Gedanken nämlich zur 1. Diskursebene zurück: Anstelle der abstrakten Zahlen wendet es sozusagen die „Definition“ an: Die Zahl 4 steht etwa für vier Äpfel und die Zahl 3 für drei Äpfel. Dann rechnet es wie auf der 1. Diskursebene und zählt die Gesamtzahl der erhaltenen Objekte ab, in diesem Fall also sieben Äpfel. Nun ist das Ergebnis ermittelt, das Kind weiß, dass 4 + 3 die Zahl 7 ergibt.

Diese Abstraktion ist charakteristisch für die 2. Diskursebene. In der Geometrie sprechen wir an Stelle von Abstraktion von der Idealisierung der vorliegenden Objekte. Zwei sich an einer Stelle berührende gerade Striche auf der Tafel werden etwa zu Geraden (unendlich dünn), welche sich in einem Punkt (unendlich klein) schneiden.

Wie lernt der Schüler bzw. die Grundschülerin das Multiplizieren? Wie bereits von der Addition bekannt, erfolgt dies wieder durch das Abzählen, etwa ist $3 \cdot 4$ genau die Zahl welcher der Anzahl der Äpfel (1. Diskursebene) in einem Rechteck aus drei Zeilen und vier Spalten entspricht:

ein Apfel	zwei Äpfel	drei Äpfel	vier Äpfel
fünf Äpfel	sechs Äpfel	sieben Äpfel	acht Äpfel
neun Äpfel	zehn Äpfel	elf Äpfel	zwölf Äpfel
drei · vier Äpfel = zwölf Äpfel			

Insgesamt lässt sich also die angeordnete algebraische Struktur der natürlichen Zahlen $(\mathbf{N}, +, \cdot, <)$ bereits auf der physikalischen Ebene begründen.

3. Diskursebene:
Nach einiger Zeit hat das Kind Erfahrungen gesammelt. Es kehrt dann beim Ausrechnen einfacher Terme nicht mehr zu den konkreten physikalischen Objekten zurück und fängt an zu zählen, stattdessen kann es das Ergebnis gleich angeben. Dieser Prozess des Sammelns von Erfahrungen kann auch erzwungen werden: So lernen Grundschüler etwa das kleine Ein-Mal-Eins auswendig, um langwierige Abzählungen zu vermeiden.
Auch weiß ein Kind nach einiger Zeit, dass in $(\mathbf{N}, +, \cdot, <)$ das sogenannte Distributivgesetz gilt, z.B. ist

$$(3 + 4) \cdot 5 = 3 \cdot 5 + 4 \cdot 5.$$

Das Kind pflegt also den Umgang mit den abstrahierten, idealisierten Objekten aus der 2. Diskursebene, verwendet hierbei aber zwar abstrakte, aber sich selbst bewusst gemachte Regeln. Es befindet sich auf der 3. Diskursebene. Diese Diskursebene wird typischerweise in der Sekundarstufe I und II verwendet, ansatzweise jedoch auch in der Primarstufe.

4. Diskursebene:
Auf der Hochschule werden die natürlichen Zahlen (einschließlich der Null) etwa wie folgt eingeführt:

$0 := |\emptyset|$,
$1 := |\{\emptyset\}|$,
$2 := |\{\emptyset, \{\emptyset\}\}|$,
$3 := |\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}|$,
...

Um diesen Zugang zu wählen, muss man aber zunächst wissen, was die leere Menge ø ist bzw. was überhaupt Mengen sind. Letzen Endes führt uns dies zu der Frage nach einem Axiomensystem. Was also sind geeignete Axiome für die natürlichen Zahlen? Was wollen wir als undefinierte Grundbegriffe verwenden? Wir könnten etwa die Additions-Operation + oder die Kleiner-Relation < verwenden. Oder etwa die charakteristische Eigenschaft der natürlichen Zahlen,

dass es zu jeder natürlichen Zahl einen „Nachfolger“ gibt, der wieder eine natürliche Zahl ist. (Bezeichnet etwa x’ den Nachfolger von x, so ist 4’ = 5.)
Dies führte Anfang des 20. Jahrhunderts zu den sogenannten Peano-Axiomen für (**N**, 1, ’).

Nun wissen wir also (auf der jeweiligen Diskursebene), was die natürlichen Zahlen sind und wie wir mit ihnen rechnen können. Im Folgenden wollen wir also den Übergang von den natürlichen Zahlen zu den ganzen Zahlen wagen.
Bekanntlich ist die Menge der ganzen Zahlen die Vereinigung aus der bekannten Menge der natürlichen Zahlen (der Menge der positiven Zahlen), der 0 und der Menge der negativen Zahlen:

$$\mathbf{Z} = \mathbf{N} \,?\, \{0\} \,?\, -\mathbf{N}.$$

„Was sind aber negative Zahlen? Wozu brauchen wir negative Zahlen und was können wir uns unter diesen vorstellen?“, würde ein Schüler der Sekundarstufe I etwa fragen.
Im Folgenden steht der unterrichtende Lehrer bzw. die unterrichtende Lehrerin vor einem Problem, denn der Gang zur 1. Diskursebene ist in diesem Fall nicht ganz einfach: Er/Sie kann die negativen Zahlen etwa an einem Thermometer oder an einem Zahlenstrahl erklären. Aber was sind etwa –3 Äpfel? Auch an Hand von Schulden (also etwas Fehlendem) oder Höhenunterschieden bezüglich einem gewählten Nullpunkt bzw. einem Fahrstuhl lassen sich die negativen Zahlen durch Beispiele aus dem alltäglichen Leben erklären.
Die letzte Möglichkeit ist, dem Kind den Umgang mit den negativen Zahlen direkt an Hand der Regeln zu erklären, ohne dass es überhaupt eine Vorstellung von den negativen Zahlen bekommt: Es bekommt dann etwa gesagt, dass

$$(-2) \cdot (-6) = +12$$

ist, weil $2 \cdot 6 = 12$ ist und „–“ mal „–“ das Zeichen „+“ ergibt.

Auf formaler Ebene werden die negativen Zahlen eingeführt als Zahlen, welche Gleichungen wie

$$5 + ? = 4$$

oder

$$3 + ? = 1$$

lösen.

Aber warum gilt nun

$$(-2) \cdot (-6) = +12$$

wirklich? Die Tatsache ist doch die, dass wir eine algebraische Struktur

$$(\mathbf{Z}, +, \cdot, <) > (\mathbf{N}, +, \cdot, <)$$

suchen, in der die gewohnten Rechenregeln für **N** gelten. Sind also etwa (–2), (–6) ? **Z**, so gilt

$$(-2) \cdot (-6) = +12,$$

aus folgendem Grund:

$$2 + (-2) = 0$$

ist die Definition von (–2); multiplizieren wir diese Gleichung nun mit (–6), so erhalten wir

$$(-12) + (-2) \cdot (-6) = 0;$$

addieren wir weiter (+12), so ergibt sich

$$(-2) \cdot (-6) = +12.$$

(Anmerkung: Wir haben hier bereits benutzt, dass $2 \cdot (-6) = -12$ ist, dies muss natürlich zuerst gezeigt werden.)

In der Schule zeigt man also, dass wir mit den ganzen Zahlen so rechnen können, wie wir es von den natürlichen Zahlen gewohnt sind. Die Frage nach der Existenz solcher Zahlen wird jedoch in der Schule nicht gestellt, man versucht die Existenz an Hand der oben genannten Beispielen zu erklären.

Wählt man wie auf der Hochschule den axiomatischen Zugang der 4. Diskursebene, so kann man die Existenz ganzer Zahlen beweisen. Per Definition sind die ganzen Zahlen solche, welche eine gewisse Sorte algebraischer Gleichungen lösen:
Zum Beispiel ist (–3) die eindeutig bestimmte Lösung der Gleichung

$$8 + ? = 5$$

und (–1) die von

$$6 + ? = 5,$$

aber auch die von

$$5 + ? = 4.$$

Wir können also sagen, das natürliche Zahlenpaar (8, 5) charakterisiert die negative Zahl (–3). Wie wir weiter sehen, ist eine solche Charakterisierung einer ganzen Zahl durch zwei natürliche Zahlen nicht eindeutig, so können wir etwa (–1) durch (6, 5) oder aber durch (5, 4) darstellen. Es ist also nicht möglich, die ganzen Zahlen durch Zahlenpaare direkt zu definieren. Stattdessen müssen wir eine Äquivalenzrelation ~ definieren, so dass etwa

$$(6, 5) \sim (5, 4)$$

ist. Weiter muss man dann zeigen, dass ~ auch eine Kongruenzrelation ist. Geht man dann über zur Faktorstruktur, so können wir die ganzen Zahlen als Äquivalenzklassen von ~ definieren.

Vor zur nächsten Stunde (16.10.03),
zurück zur Protokollübersicht.

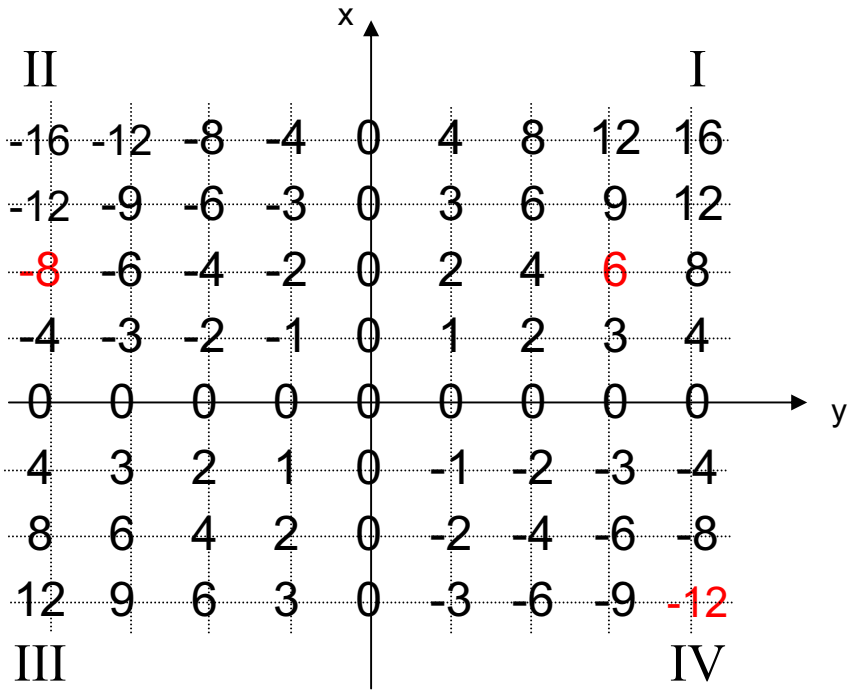
Elementare Zahlentheorie WS 03/04
Stundenprotokoll vom 16.10.2003 (RD)

[Zurück zur Protokollübersicht.]

Thema der Stunde: Die ganzen Zahlen

1. Warum ist das Produkt zweier negativer Zahlen positiv?

Zunächst haben wir noch einmal das Thema der letzten Stunde, nämlich: „Wie motiviert man, dass das Produkt zweier negativer Zahlen eine positive Zahl ergibt?“ aufgegriffen.
Dazu kann der Lehrer mit seinen Schülern zusammen eine **Multiplikationstafel** aufstellen.
Diese sieht für das Produkt x • y folgendermaßen aus:



Aber wie erhält man die Zahlen in den einzelnen Quadranten?
Im ersten und zweiten Quadranten kann der Lehrer die Multiplikation über die erste Diskursebene, d. h. anhand von physikalischen Objekten erklären.
So ergibt sich z. B. die rot markierte 6 im ersten Quadrant aus „2 mal 3“. Die Schüler können sich dazu vorstellen: „Ich habe 2mal drei Äpfel, also sechs Äpfel“.
Auch z. B. die rot markierte (-8) aus dem zweiten Quadranten lässt sich noch auf der ersten Diskursebene erklären, sie ergibt sich aus „2mal (-4)“. Dazu stellen sich die Schüler z. B. vor: „Mir fehlen 2mal 4 Äpfel, also fehlen mir insgesamt 8 Äpfel“.

Aber für die letzten beiden Abschnitte in der Multiplikationstafel fehlt den Schülern eine Anschauung.
Im vierten Quadranten stellt sich die Frage: „Was ist z. B. -3mal 4 Äpfel?“
Hier muss man von der ersten Diskursebene weggehen und mit den Regeln argumentieren, die die Schüler für die natürlichen Zahlen bereits auf der dritten Diskursebene gelernt haben.
Sie kennen unter anderem schon das Kommutativgesetz der Multiplikation für die natürlichen Zahlen. Also muss man ihnen klar machen, dass es sinnvoll ist, dass diese Regel auch bei den neuen

negativen Zahlen gelten soll. Es soll also gelten x•y = y•x. Damit kann man dann die Ergebnisse des vierten Quadranten aus denen des zweiten Quadranten ableiten.

Nun bleibt noch das Problem des dritten Quadranten, warum das Produkt von zwei negativen Zahlen positiv sein soll. Dazu muss man die Schüler auf eine gewisse Regelmäßigkeit in der Tabelle hinweisen:
Man erkennt, dass die Zahlen in der untersten Zeile des ersten Quadranten von rechts nach links gelesen immer um eine Einheit verringert werden. Dies wird auch in der untersten Zeile des zweiten Quadranten so fortgesetzt. Da in der obersten Zeile des vierten Quadranten die Zahlen von rechts nach links gesehen immer größer werden, wäre es also auch logisch, dies im dritten Quadranten so weiter fortzusetzen. Für die anderen Zeilen geht dies analog. Der Unterschied ist nur, dass die Zahlen dann immer um 2, 3, 4, … verringert bzw. vergrößert werden.

Somit ist die Multiplikationstabelle fertig aufgestellt. Sie ist zwar kein mathematischer Beweis dafür, dass „- mal -“ positiv ist, aber somit kann man den Schülern verdeutlichen, dass dies die einzig logische Möglichkeit ist, die Multiplikation auf den negativen Zahlen fortzusetzen.

2. Konstruktion der ganzen Zahlen aus den natürlichen Zahlen (4. Diskursebene)

Man kann die negativen Zahlen, wie bereits in der letzten Stunde angesprochen, als Zahlen einführen, die Gleichungen, wie z. B.: 7 + ? = 4 oder 5 + ? = 2, lösen.
Wie man sieht, wird also durch die Zahlenpaare (7, 4) und (5, 2) die gleiche negative Zahl, nämlich (-3), beschrieben.
Somit muss man eine Äquivalenzrelation definieren, so dass etwa (7, 4) ~ (5, 2) gilt.

Zur Konstruktion der ganzen Zahlen aus den natürlichen Zahlen muss man also folgende Schritte durchführen:
1) Definition einer Äquivalenzrelation [(x, y) ~ (x', y')]
2) Definition einer Äquivalenzklasse
3) Definition der Operation „+“
4) Definition von Z

Zu 1) (Definition einer Äquivalenzrelation):
Um eine geeignete Äquivalenzrelation zu definieren, muss man sich zunächst auf einem „Schmierzettel“ überlegen, wie diese aussehen sollte:
Zwei Zahlenpaare (x, y) und (x', y') sollten äquivalent zueinander sein, wenn sie die gleiche negative Zahl charakterisieren.
Angenommen, es gäbe bereits eine negative Zahl u, dann müsste (x, y) ~ (x', y') gelten, wenn die beiden Gleichungen

$$x + u = y$$
$$x' + u = y'$$

erfüllt sind.
Weiterhin angenommen, es gäbe bereits die Operation „-“, so ergibt sich:

$$[u:=]\ y - x = y' - x' \quad \text{bzw.} \quad y + x' = y' + x$$

Nun kann man die Äquivalenzrelation definieren.

Definition:
Für (x, y), (x', y') □ IN x IN schreibe (x, y) ~ (x', y'), wenn gilt: y + x' = y' + x.

Als nächstes muss man nachweisen, dass ~ tatsächlich eine Äquivalenzrelation auf IN x IN ist, d. h. man muss zeigen, dass ~ reflexiv, symmetrisch und transitiv ist.

- Reflexivität: Zu zeigen ist: (x, y) ~ (x, y)
  ~ ist reflexiv, denn es gilt y + x = y + x.

- Symmetrie: Zu zeigen ist: Aus (x, y) ~ (x', y') folgt (x', y') ~ (x, y).
  ~ ist symmetrisch, denn aus y + x' = y' + x folgt y' + x = y + x'.
- Transitivität: Zu zeigen ist: Aus (x, y) ~ (x', y') und (x',y') ~ (x'', y'') folgt (x, y) ~ (x'', y'').
  ~ ist transitiv, denn aus y +x' = y' + x und y' + x'' = y'' + x' folgt durch Addition der beiden Gleichungen:

$$y + x' + y' + x'' = y' + x + y'' + x' \text{ , also:}$$
$$y + x'' = y'' + x.$$

Zu 2) (Definition einer Äquivalenzklasse):

Definition:

Es sei ~ die oben definierte Äquivalenzrelation. Für (x, y) □ IN x IN schreiben wir:

$$(x, y)^{\sim} := \{ (x', y') \square \text{ IN x IN} \mid (x', y') \sim (x,y) \}$$

Diese „Töpfe" bilden eine Klasseneinteilung von IN x IN, d. h. die Vereinigung aller Äquivalenzklassen bildet ganz IN x IN, und die Äquivalenzklassen sind paarweise disjunkt.

Zu 3) (Definition der Operation „+"):

Um eine geeignete Definition für die Addition zu finden, muss man sich zunächst wiederum auf einem „Schmierzettel" überlegen, was diese Addition leisten soll.
Es seien (x, y) und (x', y') □ IN x IN. Es gilt also x + u = y und x' + v = y'.
Durch Addition der beiden Gleichungen erhält man: (x + x') + (u + v) = (y + y').
Also charakterisiert das Zahlenpaar (x+x', y+y') die Zahl (u+v).
Nun kann man also die Addition definieren:

Definition:

Für (x, y), (x', y') □ IN x IN setze $(x, y)^{\sim} + (x', y')^{\sim} := (x + x', y + y')^{\sim}$.

Es stellt sich die Frage, ob das repräsentantenweise Rechnen wohldefiniert ist. Dazu muss man nachweisen, dass ~ eine Kongruenzrelation ist, d. h. aus (x, y) ~ (x', y') und $(x_1, y_1) \sim (x_1', y_1')$ muss folgen $[(x, y) + (x_1, y_1)] \sim [(x', y') + (x_1', y_1')]$ für (x, y), (x', y'), (x_1, y_1), (x_1', y_1') □ IN x IN.

~ ist eine Kongruenzrelation, denn zu zeigen ist :

$$[(x, y) + (x_1, y_1)] \sim [(x', y') + (x_1', y_1')], \text{ also}$$
$$(x + x_1, y + y_1) \sim (x' + x_1', y' + y_1'), \text{ somit}$$
$$y + y_1 + x' + x_1' = y' + y_1' + x + x_1.$$

Da nach Voraussetzung (x, y) ~ (x', y') und $(x_1, y_1) \sim (x_1', y_1')$, gilt also:

$$y + x' = y' + x,$$
$$y_1 + x_1' = y_1' + x_1,$$

und somit gilt die Gleichheit der oberen beiden Terme. Also ist ~ folglich eine Kongruenzrelation und somit ist die von uns definierte Addition wohldefiniert.

Zu 4) (Definition von Z):

Definition:

$Z := \{ (x, y)^{\sim} \mid (x, y) \square \text{ IN x IN} \}$

Nun, da wir die ganzen Zahlen aus den natürlichen Zahlen konstruiert haben, stellen sich die folgenden Fragen:

1) Welchen Namen geben wir unseren Äquivalenzklassen?
2) Welche Äquivalenzklassen beschreiben die natürlichen Zahlen?

3) Welche Rechenregeln gelten für die Äquivalenzklassen? Dieselben wie in IN?
4) Besteht ein Isomorphismus zwischen IN und einer Teilmenge der Menge aller Äquivalenzklassen?
5) Welches „ist“ die Menge der „positiven Töpfe“?

Zu Frage 5):
Die Menge der „positiven Töpfe“ ist die Menge P := { (x, y) | x < y, (x, y) □ IN x IN }.

Zu Frage 4):
Wir betrachten die Abbildung j := (u → (1,u+1)˜): IN → P.
Dadurch stellen sich wieder neue Fragen:
(i) Ist j injektiv und surjektiv?
(ii) Ist j wohldefiniert?

Zurück
zur vorangehenden Stunde (14.10.03),
zur Protokollübersicht.

§ 1 Figurierte Zahlen: Anschauung und Kreativität

1. Finden sie eine Formel für Δ_n = Summe der ersten n natürlichen Zahlen!

(z.B. $1 + 2 + \ldots + \underbrace{137206}_{n}$)

Idee: Die Summe der letzten und der ersten Zahl der gegebenen Summe ergibt $(n+1)$, die Summe der vorletzten und der zweiten Zahl ergibt wieder $(n+1)$, u.s.w..

Insgesamt ergeben sich $\frac{n}{2}$ solcher Paare.

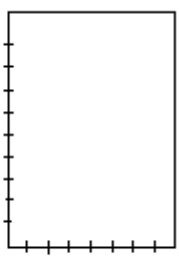
$$\rightarrow \Delta_n = \frac{n(n+1)}{2} = \frac{n}{2}(n+1)$$

Anschauung: Mit Hilfe von Kästchen lassen sich die Zahlen von 1 .. n darstellen: Die erste Spalte des 'Dreiecks' stellt die Zahl 1 dar, die zweite Spalte die Zahl 2, u.s.w..

Die Summe der gesamten Kästchen ergibt nun Δ_n .

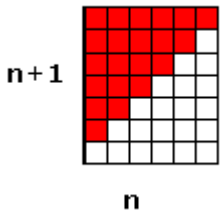
n = 6

Problem: Die Kästchen lassen sich für große n nicht mehr abzählen. Für eine Rechteck-Form wäre dies einfacher.



n

Bilde also durch Übereinanderlegen zweier Dreicks-Kästchen- Formen ein Rechteck: Es entsteht ein Rechteck mit den Seitenlängen n und n+1.



→ Formel: $\Delta_n = \frac{n}{2}(n+1)$

2. Finden sie eine Formel für U_n := Summe der ersten n ungeraden natürlichen Zahlen!

Plan: 0) Tabelle von Beispielen zur Aufstellung einer Vermutung

1) Behauptung formulieren

2) Behauptung beweisen

Schreiben:

0)

n = 1	1	= 1	= 1^2
n = 2	1 + 3	= 4	= 2^2
n = 3	1 + 3 + 5	= 9	= 3^2
n = 4	1 + 3 + 5 + 7	= 16	= 4^2
n = 5	1 + 3 + 5 + 7 + 9	= 25	= 5^2
n = 6	1 + 3 + 5 + 7 + 9 + 11	= 36	= 6^2

1) Behauptung: $U_n := n^2$.

2) Beweis per vollständiger Induktion:

Da wir die Summe der ungeraden Zahlen berechnen, ist

$a_n = 2n - 1$.

Damit ist: n = 1 √

Induktionsschritt:

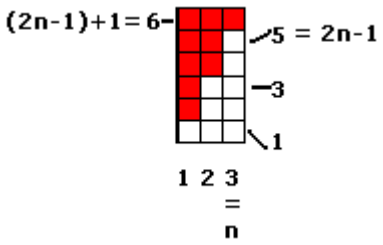
$$U_{n+1}=U_n+a_{n+1}=n^2+2(n+1)-1=n^2+2n+1=(n+1)^2$$

√

Damit haben wir nach dem Induktionsprinzip unsere Vermutung bewiesen (aber noch lange nicht verstanden)!

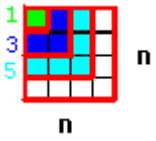
3) Anschauliche Vorstellungen:

(i) Stelle die Zahlen erneut durch Kästchen dar. Die erste Spalte in weiß gehört zu n=1, die zweite zu n=2 ... Da nur die ungeraden Zahlen summiert werden sollen, sind als n-te Spalte 2n-1 Kästchen gezeichnet. Legt man nun das 'Dreieck' noch einmal oben dran (rot), erhält man ein Rechteck der Seitenlängen n und (2n-1)+1.



→ Formel: $U_n=[(2n-1)+1]\frac{n}{2}=n^2$

(ii) Eine weitere Idee ist, die Kästchen entsprechend den Zahlen direkt zu einem Quadrat zu legen. Jede größere, ungerade Zahl ergibt ein größeres Quadrat.



Dies ergibt ein Quadrat mit der Seitenlänge n. → $U_n=n^2$

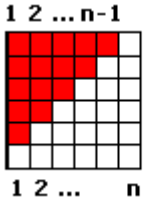
3. Finden sie eine Formel für A_n := 1+2+3+..+(n-1)+n+(n-1)..+1 (Auf-und-Ab-Regel)!

Methode: Bekannte Formel anweden: $\Delta_n=1+2+..+n$

Drücke also A_n durch Δ_n aus.

$$A_n=(1+2+3+\ldots+n)+((n-1)+\ldots+1)=\Delta_n+\Delta_{n-1}=\frac{n(n+1)}{2}+\frac{(n-1)n}{2}=\frac{1}{2}(n^2+n+n^2-n)=n^2$$

Anschauliche Vorstellung: Wie im ersten Beispiel bilden wir wieder ein Rechteck durch übereinanderlegen zweier 'Dreiecke', mit dem Unterschied, dass wir nun (da der zweite Teil der Summe A_n nur bis (n-1) geht) die Spalte für n weg lassen. Es ergibt sich also ein Quadrat der Seitenlänge n.



n^2

$\rightarrow A_n = n^2$

4. Finden sie eine Formel für Q_n := Summe der ersten n Quadrate!

$$Q_n=1+4+9+16+\ldots+n^2$$

Plan: 0) Gewinnung einer Vermutung

Methoden: a)Beispiele hinschreiben

b)Geometrische Idee

Zu a) Betrachte die Summe der Quadrate genauer: Auffällig ist, dass der Abstand zweier aufeinanderfolgender Summanden gerade die ungeraden Zahlen darstellen.

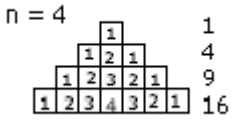
$$Q_n=\underbrace{1}_{1}+\underbrace{4}_{1+3}+\underbrace{9}_{1+3+5}+\underbrace{16}_{1+3+5+7}+\ldots+n^2$$

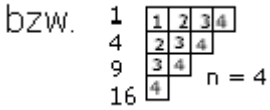
Benutze also $U_n=1+3+5+7+\ldots \rightarrow \quad b_{n+1}=b_n+a_n$

(nicht weiter verfolgt)

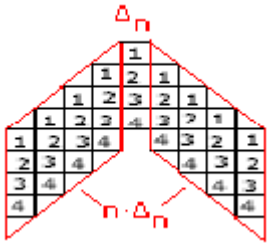
Zu b) Benutze schon bekannte Summen: $\Delta_n=1+2+..+n=\frac{n(n+1)}{2}$

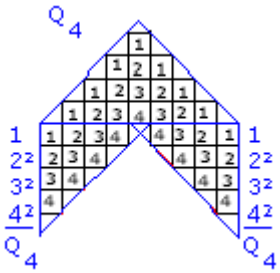
Bilde für die Summe Q_n ein Dreieck folgender Form (hier für n=4):





Setzte das zweite Dreieck nun zweimal an das erste an und erhalte einen „Pfeil", der auf zwei unterschiedliche Art und Weisen interpretiert werden kann:





Also: $3Q_n = 2n\Delta_n + \Delta_n = (2n+1)\Delta_n$

$$\rightarrow Q_n = \frac{2n+1}{3}\Delta_n = \frac{(2n+1)n(n+1)}{6}$$

5. Finden sie eine Formel für K_n := Summe der ersten n Kuben!

$$K_n = 1+2^3+3^3+4^3+\ldots+n^3$$

Methode: Bekannte Formel anwenden: $\Delta_n = 1+2+..+n = \frac{n(n+1)}{2}$

Wie in Teil 1) ist Δ_n anschaulich:

$\Delta_n =$

Multipliziert man zwei solcher Δ_n so erhält man die anschauliche Darstellung von K_n :

Multiplikationstabelle

Σ

1·1	1·2	1·3	...	1·n
2·1	2·2	2·3	...	2·n
3·1	3·2	3·3	...	3·n
...	...	...	⋱	...
n·1	n·2	n·3	...	n·n

$= K_n = (1+2+...+n)(1+2+...+n)$

$= \Delta_n^2$

Damit: $K_n = \Delta_n^2 = \frac{n^2}{4}(n+1)^2$

Nachträglicher Hinweis:
Wir haben es hier mit verschiedenen Folgen natürlicher Zahlen zu tun. Es gibt eine Internetseite The On-Line Encyclopedia of Integer Sequences von N. J. A. Sloane, die viele viele solche Folgen erkennt und erläutert. Dazu gibt es auch ein Buch von Sloane: *A Handbook of Integer Sequences*, New York: Academic Press, 1973. Ein jüngerer Artikel von Sloane über die Folgen-Datenbank steht in der Mitglieder-Zeitschrift *Notices of the American Mathematical Society* **50**:8 (2003), 912--915 mit dem Titel: The On-Line Encyclopedia of Integer Sequences.

Zurück
zur vorangehenden Stunde (16.10.03),
zur Protokollübersicht.

Elementare Zahlentheorie WS 2003/04

Stundenprotokoll vom 23.10.2003 AW

[Zurück zur Protokollübersicht.]

§2 Rechnen: Teilbarkeit und Reste in Z

§ 2 Teil A) Rechenproben:

Proben sind zwar kein Beweis für die Richtigkeit einer Rechnung, jedoch können sie eventuelle Fehler aufdecken.

Bsp: Addition zweier Zahlen

a + b = c

163 057 + 16 513 = 179 570

Ist das Ergebnis richtig? Wie kann man Proben durchführen?

- Stellenzahl abschätzen.
- Wenn a und b gerade sind, so ist auch die Summe gerade.
- Wenn a und b ungerade sind, so ist die Summe gerade.
- Wenn a gerade ist und b ungerade, so ist die Summe ungerade.
- Wenn a und b gerade sind, so ist auch das Produkt gerade.
- Wenn a und b ungerade sind, so ist auch das Produkt ungerade.
- Wenn a gerade ist und b ungerade, so ist das Produkt gerade.

Betrachte jetzt einen Ring mit zwei Elementen:

$\underline{2} := \{0, 1\}$

In diesem Ring rechnen wir „modulo 2“

Allgemein gilt: $\underline{n} := \{0, 1, ..., n-1\}$

Rechenregeln:

$x \# y = x + y \bmod n \quad \in \mathbb{Z}$
$x *_n y = x \cdot y \bmod n \quad \in \mathbb{Z}$

Warum liefert das Rechnen modulo n eine Probe?

$a + b = c \in \mathbf{Z}$

Übergang zu den Resten:

$a' = a \bmod n \in \underline{n}$
$b' = b \bmod n \in \underline{n}$
$c' = c \bmod n \in \underline{n}$

Was wird überprüft? Worin besteht die Probe?

Frage: Ist $a' \# b' = c'$?

Ja! Wenn $a + b = c$ gilt, dann gilt auch $a' \# b' = c'$.

$': (x \rightarrow x \bmod n): \mathbf{Z} \rightarrow \underline{n}$ ist Ring-m-1-Epimorphismus.

Warum ist das so?

Um diese Frage zu beantworten, benötigen wir die Beziehung zwischen x und x'. Es gilt:

Es existieren $q, n \in \mathbf{Z}$, sodass gilt: $x = qn + x'$. Denn x' ist der Rest, der bei Division durch n entsteht.

Beweis:

1. Addition: $q_c n + c' = c = a + b = (q_a n + a') + (q_b n + b')$

$= (q_a + q_b)n + (a' + b')$
$= (q_a + q_b)n + qn\ (a' \# b')$

2. Multiplikation: $q_c n + c' = c = a \cdot b = (q_a n + a') \cdot (q_b n + b')$

Ist die Darstellung einer Zahl in der Form $z = qn + z'$, $z' \in \underline{n}$ eindeutig?

Ja, bei Division mit Rest sind sowohl q als auch der Rest eindeutig bestimmt.

Es gilt also in der Tat

$$c' = a' \# b'$$

Was nützt uns diese Erkenntnis jetzt für Proben?

Betrachte die sogenannten *2-er-Probe, 3-er-Probe, 7-er- Probe, 9-er-Probe, 11-er-Probe, 13-er-Probe und 17-er-Probe:*

Betrachte hierfür die folgende Dezimalschreibweise einer Zahl $a \in \mathbf{Z}$:

$a = [a_n \ldots a_3 a_2 a_1 a_0] = a_n 10^n + \ldots + a_2 10^2 + a_1 10^1 + a_0 10^0$.

9-er-Probe:

Bildung der iterierten Quersumme:

Bsp: $281765111_9 = 5$

Bilde ich also die Quersumme von 281765111 und rechne modulo 9, erhalte ich 5.
Wenn bei dieser Vorgehensweise der Rest 0 herauskommt, ist die gegebene Zahl durch 9 teilbar.
Außerdem gilt: Wenn die 9-er Probe stimmt, dann stimmt die 3-er Probe erst recht, denn jede Zahl, die durch 9 teilbar ist, ist insbesondere durch 3 teilbar.

Beweis der Formel für den 9-er-Rest:

$a = [a_n \ldots a_3 a_2 a_1 a_0]$

$= (a_n 10^n + \ldots + a_2 10^2 + a_1 10 + a_0 1)_9$
$= (a_n)_9 + \ldots + (a_1)_9 + (a_0)_9$

11-er-Probe:

Bildung der alternierenden (iterierten) Quersumme:

Beweis der Formel für den 11-er-Rest:

$a_{11} = [a_n \dots a_3 a_2 a_1 a_0]_{11}$

$= (a_n 10^n + \dots + a_2 10^2 + a_1 10 + a_0 1)_{11}$
$= (a_n)_{11}\ 10^n{}_{11} + \dots + (a_1)_{11} 10^1{}_{11} + (a_0)_{11}\ 10^0{}_{11}$
$= (\pm 1)^n\ a_n + \dots + a_2 - a_1 + a_0$

Bsp: $281765111_{11} \equiv_{11} 1$ denn: $1 + 1 - 1 + 5 - 6 + 7 - 1 + 8 - 2 \equiv_{11} 1$

13-er-Probe:

$a_{13} = [a_n \dots a_3 a_2 a_1 a_0]_{13}$

$= (a_n 10^n + \dots + a_2 10^2 + a_1 10 + a_0 1)_{13}$
$= (a_n)_{13}\ 10^n{}_{13} + \dots + (a_1)_{13} 10^1{}_{13} + (a_0)_{13}\ 10^0{}_{13}$

Folge der Reste (d.h. Koeffizienten der jeweiligen a_i): (1, -3, -4, -1, 3, 4, 1, -3, -4, ...)

Fragen:

- Wie viele Proben sind sinnvoll? (Wie richtig ist mein Ergebnis?)
- Welche Proben sind sinnvoll oder besser?

Frage: Wenn die 2-er-Probe und die 3-er-Probe stimmt, stimmt dann auch die 6-er-Probe?

Betrachte:

$a = q \cdot 2 + a_2$
$a = q' \cdot 3 + a_3$

$a = q'' \cdot 6 + a_6$

Die letzte Zeile ergibt sich, da 2 und 3 teilerfremd sind, das heißt, dass der ggT(2, 3) = 1 ist.

Andererseits:

$a = q \cdot 2 + a_2$
$a = q' \cdot 4 + a_4$

$a = q'' \cdot 4 + a_4$

Die letzte Zeile ergibt sich, da 2 und 4 nicht teilerfremd sind. Man würde vielleicht in der dritten Zeile die 8 erwarten, betrachte jedoch hierzu folgendes Gegenbeispiel:

2 teilt 4 und 4 teilt 4, jedoch teilt 8 nicht 4.

(Für den Beweis, dass aus der Richtigkeit der 2-er- und der 3-er-Probe die Richtigkeit der 6-er-Probe folgt, siehe Protokoll vom 24.10.2003)

Zurück
zur vorangehenden Stunde (21.10.03),
zur nächsten Stunde (24.10.03),
zur Protokollübersicht.

Elementare Zahlentheorie WS 2003/04

Protokoll vom 24.10.2003 (TF)
(Fortsetzung von § 2 Teil A) Rechenproben. Anschließend Teil B) Strukturfragen.)

[Zurück zur Protokollübersicht.]

Konventionen: x^0 bezeichnet den „Topf“ bezüglich x.
$/Z$ bezeichnet die Menge der „Ganzen Zahlen“.
x_k bezeichnet den Repräsentanten r mit $0 < r < k$ der Restklasse $x + k\,/Z$, also $r = x \bmod k$.

Ausgangsthematik waren Zahlenproben, etwa die Proben *mod 2, mod 3, mod 4*, etc.

Kann man etwa bei gegebener Zahl a und bekannten a_2 und a_3 auf a_6 schließen?
Ist das a_6 festgelegt? Gibt es eine Formel aus a_2 und a_3?

Beispiele:

a_2	a_3	a_6
0	0	0
0	1	4
1	0	3
1	2	5
0	2	2
1	1	1

Es sei
$a = q \cdot 2 + a_2$, $b = q' \cdot 2 + b_2$,
$a = r \cdot 3 + a_3$, $b = r' \cdot 3 + b_3$
für gewisse q, q', r, r' *?/Z.*

Folgt $a_6 = b_6$, *wenn $a_2 = b_2$ und $a_3 = b_3$ ist?*

($a = s \cdot 6 + a_6$, $b = s \cdot 6 + b_6$)

$a - b = (q - q') \cdot 2$
$a - b = (r - r') \cdot 3$

$a - b = t \cdot 6$ (Hier wird stillschweigend die Eindeutigkeit der Primfaktorzerlegung genutzt.)

✌●♦□ ♓♦♦ $(a - b)_6 = 0$, $a_6 - b_6 = 0$, $a_6 = b_6$. Also ist a_6 festgelegt.

Gibt es eine Formel für a_6? Zu geg. a_2, a_3 finde b *?/Z* mit $b_2 = a_2$ und $b_3 = a_3$.

Ansatz:
Es sei $b = 2\, a_3\, x + 3\, a_2\, y$. (Lagrange)
Gesucht sind $x, y \,?/Z$, so dass für $b := 2\, x\, a_3 + 3\, y\, a_2$ gilt:
$b_2 = a_2$ und $b_3 = a_3$.

Wegen des Ansatzes ist $b_2 = 0 + (3\, y\, a_2)_2 = (3y)_2\, a_2$. Wir suchen also ein y mit $(3y)_2 = 1$.
Entsprechend suchen wir ein x mit $(2x)_3 = 1$.
Allgemeines Problem: Gegeben der Restering $\underline{n} = \{0, 1, 2, 3, \ldots, m, \ldots, (n-1)\}$. Welche Elemente m sind invertierbar: d. h. für welche m □ $/Z$ existiert ein x □ $/Z$ mit $x_n\, m_n = 1$?

Antwort. Bei teilerfremden $m, n \,?/Z$ existiert ein x mit $(x\, m)_n = 1$, also $(x_n\, m_n) = 1$.

Denn die Berechnung des *ggT g* von m und n (in $/Z$) erfolgt über den Euklidischen Algorithmus und den Erweiterten Euklidischen Algorithmus *XEA*: Es existiert eine Darstellung von g mit:

$g = u\, m + v\, n$.

Bei uns ist $g = 1 = u\, m + v\, n \;\; (u, v \,?/Z)$.
Also $1 = u_n\, m_n + 0$. $\rightarrow (2\, x)_3 = 1 = (3\, y)_2$.

Diese Lösung des allgemeinen Problems liefert speziell die Existenz von x und y mit $(2\, x)_3 = 1 = (3\, y)_2$, wie im Ansatz für die obige **Formel** gewünscht. Das Ergebnis ist der folgende Satz.

Chinesischer Restesatz:

Sind m und n teilerfremd in *IN* und sind r und $s \,?/Z$, so existiert ein $b \,?/Z$ mit $b_m = r_m$ und $b_n = s_n$.

Zusatz:

Man erhält ein solches b in der Form $b = n\, u\, r_m + m\, v\, s_n$, wenn $1 = v\, m + u\, n$ *(XEA)* gilt.

Anwendung auf Rechenproben:

Wenn $m_1, \ldots, m_r$ paarweise teilerfremd sind und die Proben *mod* $m_1, \ldots,$ *mod* m_r „stimmen“, dann stimmt das Ergebnis *mod* $m_1 \ldots m_r$.

B) Allgemeine Strukturfragen an die Ringe-m-1 der Form $\underline{n}$.

Für $a \,?\, \underline{n}$ schreiben wir $\{x \mid x \,?/Z,\, x_n = a\} =: a^0$. Es ist also $a^0 = a + n\, /Z$.

Offenbar gilt $/Z = ?_{a\, ?/Z}\, a^0$.

Hilfssatz. $a^0 \pm b^0 := (a \pm b)^0$ ist wohldefiniert.

Zum Beweis sei $a^0 = (a')^0$. [Z.z.: $(a' + b)^0 = (a + b)^0$.] Also $n \mid a' - b$. [Z.z.: $n \mid (a + b) - (a' + b)$.]

Deshalb $n \mid (a' + b) - (a + b)$, also $(a' + b)^0 = (a + b)^0$.

Hilfssatz. $a^0 \dot{-} b^0 = (a\ b)^0$ ist wohldefiniert. (Beweis selbst.)

Wir schreiben ab jetzt $+, \cdot$ statt $\dot{+}, \dot{-}$.

$n\mathbb{Z} < \mathbb{Z}$ (Gruppe bezüglich $(+, 0, -)$).

$\mathbb{Z}/n\mathbb{Z} := \{m + n\mathbb{Z} \mid m \in \mathbb{Z}\}$
$+, 0, -$ $\quad m^0$
$\cdot, 1$ $\quad -m^0 = (-m)^0$
Ring-m-1
$E(\mathbb{Z}/n\mathbb{Z}) = \{x^0 \mid x \in \mathbb{Z}$, es existiert ein y^0 mit $x^0 \cdot y^0 = 1\}$ ist Gruppe bzgl. $\cdot$
(„Einheitengruppe“)

$= \{m^0 \mid ggT(m, n) = 1\}$

$= (?)$

Beispiel: $n = 6$:

$\mathbb{Z}/6\mathbb{Z} = \{0^0, 1^0, 2^0, 3^0, 4^0, 5^0\}$. In diesem Ring-mit-1 ist 2^0 keine Einheit.

Denn es ist $2^0 \cdot 3^0 = 6^0 = 0$. Wäre nun $2^0 \cdot x^0 = 1^0$, so folgte

$0 = 3^0 \cdot 2^0 \cdot x^0 = 3^0 \cdot 1^0 = 3^0$, ein Widerspruch.

Zurück
zur vorangehenden Stunde (23.10.03),
zur nächsten Stunde (28.10.03),
zur Protokollübersicht.

Stundenprotokoll zur Vorlesung
Elementare Zahlentheorie vom 28.10.2003

[Zurück zur Protokollübersicht.]

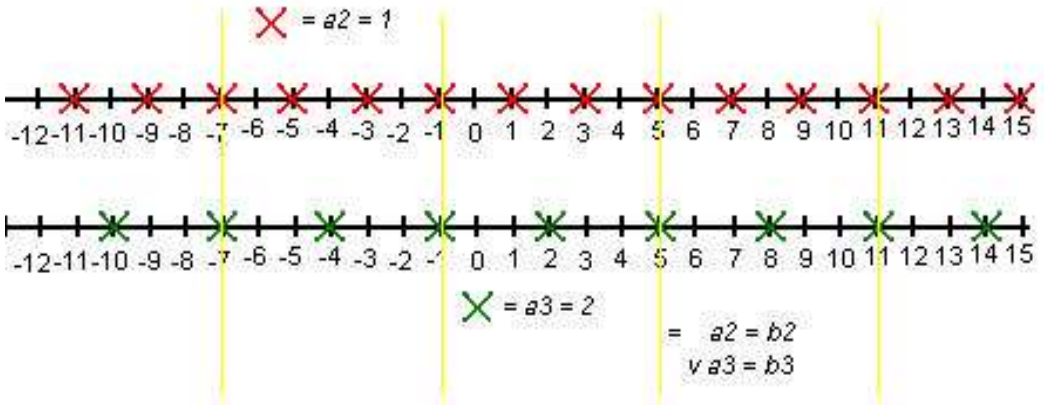
Nachtrag zum §2 A. : Rechenproben

Veranschaulichung

Wir waren von dem Problem der Teilbarkeit mit Rest von einer Zahl $a \in \mathbb{Z}$ bzgl. zweier anderer $n, m \in \mathbb{N}$ zu der Frage gekommen, welche Zahl(en) b die selben Reste bei der Division durch n und m haben. Über diese Frage haben wir den Chinesischen Restesatz hergeleitet, der uns darauf eine Antwort lieferte. Weiter wollten wir eine Aussage treffen, inwiefern man von diesen Resten auf den Rest bei der Division durch das Produkt $n \cdot m$ schließen kann.

Hier ist aber auch noch mal eine geometrische Veranschaulichung dieser Fragestellung angebracht, was in einer Schulklasse sicher vom methodischen Vorgehen im Unterricht her als das bessere Ergebnis anzusehen ist als ein abstrakter mathematischer Satz .

Es gilt z. B.
$a = nq_2 + a_2$ und $a = mq_3 + a_3$ für $a = 5, a_2 = 1, a_3 = 2$.
Welche b haben ebenfalls den Rest 1 mod 2 und den Rest 2 mod 3?
Haben sie *alle* den selben Rest mod $2 \times 3 = 6$?



Als Ergebnis folgt, auch für Schüler der unteren Jahrgangsstufen, leicht die Menge:

$$\{ b \mid a_2 = b_2, a_3 = b_3 \} = a + 6 \mathbb{Z} = \bar{a},$$
$$d.h.\ a_6 = b_6 \text{ für alle diese } b.$$

Das wird wohl nicht nur in diesem Beispiel so sein.

Chinesischer Restesatz

Wir definieren auf den Grundlagen des Chinesischen Restesatzes eine "neue" Abbildung, um die entstandene Menge(n) vielleicht über die Eigenschaften der Abbildung besser zu charakterisieren.

mod m *: = (a ? a_m): /Z ? $\underline{m}$*

bzw. ***mod m*** *: = (a ? ¯a) /Z ? /Z / m/Z,*

wobei $\underline{m}$*:={0, 1,..., n - 1} ? /Z / m/Z := {¯a| a* in */Z}* ist vermöge

$$x \ ? \ ^{-}x = x + m/Z.$$

Die Abbildung *mod m* ist surjektiv und ein wohldefinierter Ring-m-1-Homomorphismus.

Bei uns sind aber die Reste bezgl. zweier Moduln m_1 *und* m_2 (im Beispiel 2 und 3) gegeben. Aus ihnen machen wir das Paar

$$(a_{m_1}, a_{m_2}) \ ? \ (a + m_1/Z, a + m_2/Z)$$

in

$$\underline{m_1} \times \underline{m_2} \ ? \ /Z / m_1/Z \times /Z / m_2/Z.$$

Dies wirft sofort die **Frage** auf: **Ist $\underline{m_1} \times \underline{m_2}$ wieder ein Ring-m-1?**

Ja, was leicht über die komponentenweisen Operationen zu beweisen ist.

Jetzt erhalten wir den Ring-m-1-Homomorphismus
$f := (a \ ? \ (a_{m_1,} \ a_{m_2})): \ /Z \ ? \ R := (\underline{m_1} \times \underline{m_2}) \ ? \ /Z / m_1/Z \times /Z / m_2/Z.$

Ein kurzes Beispiel zum Rechnen in *R*:

$$(1, 1)\cdot (1, 2) = (1, 2)$$

$$(1, 0)\cdot (0, 2) = (0, 0)$$

Hier sind sowohl *(1, 0)* als auch *(0, 2)* ungleich Null in $\underline{m_1} \times \underline{m_2}$; trotzdem ergeben sie als Produkt das Nullelement des Ringes. Solche Ringelemente nennt man **Nullteiler**.

Frage: Sind Nullteiler multiplikativ invertierbar? Nein.

Beweis: Es sei *R* ein Ring-m-1, $a \cdot b = 0, a, b \ ? \ R, a \ ? \ 0, b \ ? \ 0.$ Angenommen *a* wäre invertierbar, dann würde gelten $x \cdot a = 1,$

mit $a \cdot b = 0 \qquad | \cdot x$

$x \cdot a \cdot b = x \cdot 0$

$1 \cdot b = b = 0$, dies ist jedoch ein Widerspruch zu $b \; ? \; 0$.

Frage: Wie und was ist das *Bild f* ?

Frage: Wie und was ist der *Kern f* ?

Bild f ist ein Unter-Ring-m-1. Aber wir wollen uns zuerst den *Kern f* genauer anschauen.

Kern f := $\{z \; ? \; /Z \mid f(z) = 0\}$ ist ein Unterring (ohne 1!).
Aus $f(z) = 0$ folgt, weil f ein Homomorphismus ist,
$f(z \cdot z') = f(z) \cdot f(z') = 0 \cdot "*" = 0$ für *alle z'* in /Z.
Der *Kern f* ist ein **Ideal** des Ringes.

Kern f $= \{z \; ? \; /Z \mid m_1 \mid z \text{ und } m_2 \mid z\} = \{z \; ? \; /Z \mid kgv(m_1, m_2) \mid z\}$.
Kern f $= \{z \; ? \; /Z \mid m_1 \cdot m_2 \mid z\} = m_1 \cdot m_2 /Z$, wenn m_1 und m_2 teilerfremd sind.

Frage: Ist *f* surjektiv? Vielleicht nur/auch, wenn m_1 und m_2 teilerfremd sind?

Um uns der Frage klarer zu werden, formulieren wir sie um und werden uns der Definitionen und Begriffe der Frage bewusst.

Existiert zu jedem $(a_1, a_2) \; ? \; R = \underline{m}_1 \times \underline{m}_2 \; ? \; /Z / m_1 /Z \times /Z / m_2 /Z$ ein $b \; ? \; /Z$
mit $a_1 = b + m_1 /Z$ und $a_2 = b + m_2 /Z$,
also mit

$$b_{m_1} = a_1 \text{ und } b_{m_2} = a_2 \text{ für } a_1 = a_1 + m_1 /Z \text{ und } a_2 = a_2 + m_2 /Z?$$

Antwort: Ja.
Der Homomorphiesatz liefert für einen Ring-m-1-Homomorphismus f einen *Isomorphismus*

$$/Z / Kern\, f \; ? \; Bild\, f,$$

$$? := (\bar{}z = z + Kern\, f \; ? \; f(z)) : /Z / Kern\, f \; ? \; Bild\, f.$$

Unser f aus dem Chinesischen Restesatz liefert uns den Isomorphismus

$$? : /Z / m_1 \cdot m_1 /Z \; ? \; /Z / m_1 /Z \times /Z / m_2 /Z,$$

denn f : $/Z \; ? \; /Z / m_1 /Z \times /Z / m_2 /Z$

§2 B. Strukturfragen an */Z / m/Z ? m*

Frage 1: Welche Elemente sind multiplikativ invertierbar?
Die multiplikativ inversen Elemente sind die sogenannten "Einheiten" von */Z / m/Z.*

Frage 2: Ist *E(/Z / m/Z)* := Menge aller multiplikativ invertierbaren Elemente eine "anständige" Menge?

"Anständig" heißt hier: Ist *E(/Z / m/Z)* ein Körper? Nein, Körper besitzen keine Nullteiler. Ist es dann vielleicht eine multiplikative Gruppe?

Zu Frage 1:
In */Z / 6/Z* ist $x = \bar{}0, \bar{}2, \bar{}3, \bar{}4$ nicht invertierbar, denn $\bar{}2 \cdot \bar{}3 = \bar{}0$;
aber die Elemente von $\{\bar{}1, \bar{}5\} = E(/Z / 6/Z)$ sind invertierbar.

In */Z / 7/Z* ist $y = \bar{}1, \bar{}2, \bar{}3, \bar{}4, \bar{}5, \bar{}6$ invertierbar, denn für a, m teilerfremd gilt $ggT(a, m) = 1$, und der *XEA* liefert uns eine Darstellung $1 = a \cdot u + m \cdot v$,
aus $\bar{}1 = \bar{}a \cdot \bar{}u + \bar{}m \cdot \bar{}v$ in */Z / m/Z* folgt also,
$\bar{}1 = \bar{}a \cdot \bar{}u$, damit ist $\bar{}u = \bar{}a^{-1}$.

Nun sei $g = ggT(a, m)$.
Daraus folgt, dass $a = g \cdot a'$ und $m = g \cdot m'$ mit a, a' und $m' \neq 0$.
$\bar{}a \cdot \bar{}m' = \bar{}(m' \cdot g \cdot a') = \bar{}(m \cdot a') = \bar{}m \cdot \bar{}a' = \bar{}0 \cdot \bar{}a' = \bar{}0$

Somit folgt also: wenn der $ggT(a, m) \neq 1$ ist, ist a ein Nullteiler und somit nicht invertierbar.

Fazit:
Somit ist $E(/Z / m/Z) = \{ \bar{}a \mid 0 < a < m, ggT(a, m) = 1\}$ die Menge der Einheiten.

f [mit $f(m) = |E(/Z / m/Z)|$] nennt man die *eulersche f-Funktion*.

Zurück
zur vorangehenden Stunde (24.10.03),
zur nächsten Stunde (30.10.03),
zur Protokollübersicht.

Elementare Zahlentheorie WS 03/04
Protokoll vom Do 30.10.03 AG
[Zurück zur Protokollübersicht]

Besprechung der Hausaufgabe vom 24.10.03: Figurierte Zahlen

Aufgabenstellung: Wählen Sie aus dem Literaturverzeichnis zur Elementaren Zahlentheorie unter Figurierte Zahlen eine Quelle aus, aus der Sie einen interessanten Punkt auswählen und auf einer halben Seite darstellen.

1.Frage: Was ist an den Figurierten Zahlen didaktisch wertvoll?

Als eine Auflockerung zum Unterrichtbeginn kann man die Fig. Zahlen verwenden, denn man kann diese auf allen vier Diskursebenen besprechen.
Gibt es noch andere Ziele, die man durch die Behandlung der Figurierten Zahlen verfolgen kann?

2. Frage: Geht es in der Schule um Inhalte oder Methoden? Soll der Lehrer den Schülern Begründungen geben oder nicht?

Durch eine geometrische Darstellung könnte der Lehrer die bildliche Vorstellung der Schüler fördern. Dies ist unter anderem auch eine Art der Begründung und zwar auf der bildlichen Ebene. Durch Kontinuität verfestigt sich das neu erworbene Wissen des Schülers. Der Lehrer sollte den Schülern mehrere Begründungen liefern, damit die verschiedenen Systeme geistiger Vorstellungen der Schüler angesprochen werden.

Aber es gibt einige Sachverhalte, die wir nicht mehr hinterfragen so wie das Zählen zum Beispiel. Auf der ersten Diskursebene lernen die Kinder das Zählen mit Äpfeln und Birnen. Man hat einen Apfel und noch einen Apfel und insgesammt hat man dann zwei Äpfel. Dann lässt man die Äpfel weg und rechnet nur noch mit Zahlen und glaubt die Begründung dafür zu haben, warum eins und eins zwei ergibt. Das bedeutet, dass die Kinder die Sprache akzeptiert haben und das Zählen auch, aber das ist noch keine Garantie dafür, dass sie mit den Zahlen ohne Probleme rechnen können.
So stellt man fest, dass die Fächer Mathematik und Biologie, die auf den ersten Blick ganz verschieden sind, sich doch gar sehr ähneln, da beiden zunächst konkrete Objekte betrachten und dann eine Theorie (natürlich nicht die gleiche) dazu konstruieren.

Man stellt eine Hypothese auf und versucht diese durch eine Theorie zu begründen. Das heisst, die Theorie ist das Ziel jeder Wissenschaft.

3.Frage: Würde jahrelanges Begründen helfen? Soll man nur spezielle Begründungen lernen oder allgemeine?

Wie es ein altes Sprichwort besagt: Übung macht den Meister. Das Begründen muss gelernt werden am besten durch eigenständige Arbeit, wobei der Lehrer nur als ein (allwissender) Berater zur Seite steht. Das richtige Lesen und Schreiben spielt in diesem Zusammenhang eine entscheidende Rolle. Doch dabei entsteht ein Problem für den Lehrer, nämlich die Prioritäten zu setzen und zwar entweder auf den Inhalt (wenig Begründung, nur das Nötigste) oder auf die Begründung (Gefahr: man schafft den vorgesehenen inhaltlichen Stoff nicht in einem vorgegebenen Zeitrahmen).

3.1 Frage: Ist Begründen wertvoll?

Der Schüler kann mit einem begründeten Sachverhalt besser umgehen als mit einem, der vom-himmel-gefallen ist und wo der Lehrer sagt, dass dieser stimmt. Wie oben schon erwähnt, soll der Lehrer dem Schüler mehrere Möglichkeiten zeigen, damit dieser die Begründung in sein eigenes

Verständnis der Mathematik einfügen kann. Der neue Stoff wird mit dem alten in Verbindung gesetzt, d.h. man hat gelernt.

3.2. Frage: Was ist der Sinn einer Begründung?

Die Richtigkeit einer Aussage wird festgestellt. Der Sachverhalt wird außerdem in einen sinnvollen (eben begündeten) Zusammenhang gestellt (so dass man ihn auch merken kann).

3.3 Frage: Geht es in der Elementaren Zahlentheorie um den Inhalt oder ums Begründen?

Man lernt Methoden kennen, die einem helfen den Inhalt zu vermitteln, und gleichzeitig erwirbt man die (didaktische) Fähigkeit, Sachverhalte zu begründen und damit wieder (s. o.), die Inhalte zu behalten.

4. Frage: Sind Figurierte Zahlen dazu geeignet, die Vollständige Induktion zu erklären?

Das Prinzip der Voll. Ind. ist es, zwei Aussagen zu beweisen, die Verankerung und den Induktionsschritt: gilt die Aussage für n, so gilt diese auch für $n + 1$.
Man kann dieses Beweisprinzip an mehreren Beispielen erklären, und dann hat sowohl der Lehrer als auch der Schüler die Sicherheit, dass die Aussage korrekt ist oder nicht.
Durch die Induktion wird eine Verbindung zur Vorstellung beim Schüler hergestellt.

Ein Beweisprinzip, das äquivalent zur Vollständigen Induktion ist:
Indirekter Beweis:
Es gibt ein n, für das die Aussage nicht stimmt. Man wählt dann den sogenannten "kleinsten Verbrecher", also das kleinste n, für das die Aussage nicht gilt. Das Prinzip des kleinsten Verbrechers stellt so sicher, dass die Aussage für alle kleineren n gilt! Das hilft bei der Produktion des gewünschten Widerspruches im indirekten Beweis.

Fazit:

Figurierte Zahlen eignen sich vor allem gut dazu, um von einer bildlichen Vorstellung auf eine Formel zu kommen. Gleichzeitg lernt man den Übergang zwischen zwei verschiedenen Darstellungsformen. Denn eine Formel ist immer präziser als ein Bild.
Als Lehrer sollte man in der Lage sein, klassengerechte Erklärungen zu geben.
Zum Beispiel:
Unterere Stufen: Bildchen
Obere Stufen: Induktion

Zurück
zur vorangehenden Stunde (28.10.03),
zur nächsten Stunde (31.10.03),
zur Protokollübersicht.

Elementare Zahlentheorie WS 2003/04

Stundenprotokoll von Freitag, dem 31.10.2003 (MH)

Thema: Restklassenringe $\mathbb{Z}/n\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z} = \{\overline{x} = x + n\mathbb{Z} \mid x \in \mathbb{Z}\},\ n \in \mathbb{N} \cup \{0\}$ (Menge aller „Töpfe")

1. Frage: Algebraische Struktur?

2. Frage: Anzahl der Elemente?

3. Frage: Erzeugendensystem?

Ad 1.:

$\mathbb{Z}: \quad +, 0, -, \cdot, 1$

Die algebraische Struktur dieser Menge ist ein kommutativer Ring-mit-1. Es bleibt die Frage zu beantworten, ob man auch mit den „Töpfen" rechnen kann.

$\overline{x} + \overline{y} := \overline{x + y}$ Wohldefiniert.

$\overline{x} \cdot \overline{y} := \overline{x \cdot y}$ Wohldefiniert.

$\overline{x} + \overline{0} := \overline{x + 0} = \overline{x}$
$\overline{x} \cdot \overline{1} := \overline{x \cdot 1} = \overline{x}$

Auch das Inverse ist wohldefiniert.

Alle Gesetze, wie z.B. das Assoziativgesetz, sind erfüllt, da sie auch in $\mathbb{Z}$ gelten.

Es handelt sich bei der Menge um eine additive Struktur: kommutative Gruppe.

Insbesondere additiv geschrieben ab jetzt.

Ad 2.:

$\mathbb{Z}_n = additive\,Gruppe\ \mathbb{Z}/\ n\mathbb{Z}$.

$|\mathbb{Z}_n| = n$, d.h. dass die Gruppe *n* Elemente hat ($\overline{0}$ *bis* $\overline{n-1}$).

Ad 3.:

Es ist die Frage zu klären, ob ein Element zur Erzeugung der Gruppe reichen würde? Wie sähe das Erzeugnis eines einzigen Elementes aus?

Unsere Überlegung geht dahin, dass die „1" als Erzeuger in Frage kommt, und dann wäre das Erzeugnis die Menge aller Vielfachen von „1". Jedoch kommt schnell die Frage nach der Erzeugung der „0" durch die „1". Ist die Erzeugung der „0" möglich, wenn nur die „1" voranden ist?

Unsere Antwort lautet, dass auch der „Nulltopf $\overline{0}$ " als Vielfaches von „1" darstellbar ist: $\overline{0} = \overline{0} \cdot 1$.

Außerdem geht es um das Gruppenerzeugnis, was per Definition unter allen Operationen -- der nullstelligen Operation *n*, die als Wert das neutrale Element 0 hat; der einstelligen Operation *i*, die jedem Element *g* sein Inverses -*g* zuordnet, und der zweistelligen Gruppenoperation (hier +) -- abgeschlossen ist; das neutrale Element liegt also immer im Gruppenerzeugnis.

Wir stellen fest: $x = x \cdot \overline{1} = \overline{1} + \overline{1} + \ldots + \overline{1}$, das heißt, der „Eins-Topf $\overline{1}$ " wird so oft addiert, wie es das x angibt, wenn x eine natürliche Zahl oder 0 ist. Wenn es negativ ist, so wird ein „-" - Zeichen geschrieben.

Somit lässt sich abschließend feststellen: $\mathbb{Z}_n = \langle \overline{1} \rangle = \langle \overline{y} \rangle$. Die additive Gruppe ist also zyklisch und wird von der „1" erzeugt.

Jetzt haben wir die Frage geklärt, ob die Gruppe von nur einem Element erzeugt werden kann. Es stellt sich jedoch erneut eine Frage. Unser Interesse gilt allen Zahlen, die auch die Gruppe erzeugen könnten. Wir suchen also andere Elemente $\overline{y}$, die auch die Gruppe erzeugen.

$\overline{y} = y \cdot \overline{1}$ $(y \in \mathbb{Z},\ y \in \{0, \ldots, n-1\})$, z.B. $(n-1) \cdot \overline{1} = -1 = \overline{y}$, d.h. wir können feststellen, dass auch das Inverse des „Erzeugers" erzeugt die ganze Gruppe.

Wir machen uns Gedanken darüber, nach welcher Methode wir unsere Frage beantworten können, und überlegen uns zwei verschiedene Strategien. Der erste Vorschlag ist das ganze theoretisch aufzubauen, die zweite Idee ist, es erst einmal mit Beispielen zu versuchen.

Der zweite Vorschlag wird dann auch in die Tat umgesetzt:

Beispiel n = 10, $\mathbb{Z}_{10} = \{\overline{0}, \ldots, \overline{9}\}$

Um der Frage nach den Erzeugern in diesem System nachzugehen, schließt sich an die Frontaldiskussion eine Arbeitsphase an, in der die Elemente der angegebenen Beispielmenge auf ihre Erzeugerfähigkeit überprüft werden.

Ergebnis dieser Arbeit:

Erzeuger: $\overline{1},\ \overline{3},\ \overline{7},\ \overline{9}$

Nicht-Erzeuger: $\overline{0},\ \overline{2},\ \overline{4},\ \overline{5},\ \overline{6},\ \overline{8}$.

Nach dieser Feststellung bleibt die Überlegung für eine allgemeine Formulierung.

Allgemeine Formulierung: $\overline{y}$ ist ein Erzeuger der zyklischen Gruppe $\mathbb{Z}_n$ genau dann, wenn ggT(y, n) = 1 ist.

Anschließend soll diese allgemeine Formulierung bewiesen werden, ebenfalls wieder in Gruppenarbeit.

Beweis:

„<=" XEA ergibt, dass $1 = ay + bn$, wobei *a, b* ganze Zahlen sind;

$\overline{1} = \overline{ay} + \overline{bn}$, daraus folgt

$$\overline{1} = \overline{ay} = \overline{a} \cdot \overline{y} = a \cdot \overline{1} \cdot \overline{y} = a \cdot (\overline{1} \cdot \overline{y}) = a \cdot (\overline{1y}) = a \cdot \overline{y} \ ,$$

somit wissen wir, dass wir die $\overline{1}$ mittels $\overline{y}$ erzeugen können. Da aber eben schon herausgefunden wurde, dass $\overline{1}$ Erzeuger der Gruppe ist, folgt die Behauptung, dass $\overline{y}$ Erzeuger ist.

„=>" Dieser Beweis geht quasi rückwärts, da *y* und *n* teilerfremd sind.

Bisher haben wir die additiv geschriebene zyklische Gruppe betrachtet. Ab jetzt wollen wir auch die multiplikative Gruppe betrachten.

$$\{\overline{0},\ \ldots,\ \overline{n-1}\} = \mathbb{Z}_{+\,n} \ \textit{isomorph}\ \ C_n = \langle e \rangle (\textit{Erzeuger}) = \{e^i \mid i \in \mathbb{Z}\} := \{e^0,\ e^1,\ \ldots,\ e^{n-1}\}$$

In der additiven Schreibweise war 0 das neutrale Element, jetzt ist diese Aufgabe der 1 zugeordnet. $e^i = 1 \ \textit{für}\ i \in n\mathbb{Z}$ (Vielfache von n).

Es gibt also einen Übergang von der additiven zur multiplikativen Schreibweise:

$$(\overline{x} \to e^{x}) \underset{\leftarrow Logarithmieren}{\overset{\rightarrow Exponentieren}{}} (\overline{x} + \overline{y} \to e^{x+y})$$

Es handelt sich also bei der multiplikativen und der additiven Gruppe um isomorphe Gruppen bzgl. zweier zueinander inverser Isomorphismen.

Dies beantwortet auch die Frage, wie die weiteren Erzeuger der (multiplikativ geschriebenen) zyklischen Gruppe aussehen:
$C_n = \langle e^{y} \rangle$ *für* (y, n) *teilerfremd* (analog zur Addition).

Wir betrachten nun die multiplikative Struktur von $\mathbb{Z}/n\mathbb{Z}$: Multiplikation, 1

4. Frage: Typ?

Bei dieser Menge handelt es sich um einen Monoid.

5. Frage: Welche Elemente sind invertierbar im Monoid?
$E(\mathbb{Z}/n\mathbb{Z}) = Menge\,der\,Einheiten = \{\overline{x} \mid x \in \mathbb{Z}, (x,n)\ teilerfremd\}$, also die Menge aller „Töpfe" die durch zu *n* teilerfremde Elemente repräsentiert werden.

Denn: $\overline{1} = \overline{x} \cdot \overline{u}, \quad wenn\ 1 = xu + nv \quad (nach\ XEA\ Darstellung\ der\ 1)$

6. Frage: Was für eine Struktur hat $E(\mathbb{Z}/n\mathbb{Z})$?

--> abgeschlossen unter Multiplikation: $\overline{x} \cdot \overline{x'} = \overline{1}$

$\overline{y} \cdot \overline{y'} = \overline{1}$

Produkt ist auch invertierbar

--> Eins invertierbar => Monoid

--> jedes Element ist invertierbar => Gruppe

7. Frage: Wieviele Elemente hat diese Menge?

$|E(\mathbb{Z}/n\mathbb{Z})| =: \varphi(n) \quad Eulersche\ Phi-Funktion$

8. Frage: Wir haben noch keine explizite Formel. Wie sieht also die/eine Formel für diese Euler-Funktion aus?

Um diese Frage zu beantworten, wurde etwas diskutiert und im Anschluss daran wieder ein Beispiel vorgeschlagen. Als Ergebnis dieser Arbeitsphase wurde folgende Tabelle an der Tafel festgehalten:

n	$\lvert\mathbb{Z}/\ n\mathbb{Z}\rvert$	$\lvert E(\mathbb{Z}/\ n\mathbb{Z})\rvert$	$E(\mathbb{Z}/\ n\mathbb{Z})$
1	1	1	$\{\overline{1}\}$
2	2	1	$\{\overline{1}\}$
3	3	2	$\{\overline{1},\ \overline{2}\}$
4	4	2	$\{\overline{1},\ \overline{3}\}$
5	5	4	$\{\overline{1},\ \overline{2},\ \overline{3},\ \overline{4}\}$
6	6	2	$\{\overline{1},\ \overline{5}\}$
7	7	6	$\{\overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5},\ \overline{6}\}$
8	8	4	$\{\overline{1},\ \overline{3},\ \overline{5},\ \overline{7}\}$
9	9	6	$\{\overline{1},\ \overline{2},\ \overline{4},\ \overline{5},\ \overline{7},\ \overline{8}\}$
10	10	4	$\{\overline{1},\ \overline{3},\ \overline{7},\ \overline{9}\}$

[Ab hier muss noch redigiert werden.]

Überlegungen zur Findung der Formel:

--> $6 = 2 \cdot 3$ $\quad 2 = 1 \cdot 2$ funktioniert, aber

$9 = 3 \cdot 3$ $\quad 6 \neq 2 \cdot 2$ funktioniert nicht!

--> Wenn n eine Primzahl ist, so ist $\varphi(p) = p - 1$, p: Primzahl

--> Chinesischer Restesatz:

$\mathbb{Z}/\ n_1 \cdot n_2\mathbb{Z}$ *isomorph* $\mathbb{Z}/\ n_1\mathbb{Z}\ x\ \mathbb{Z}/\ n_2\mathbb{Z}$, *falls* n_1, n_2 *teilerfren*

Sie sind isomorph bezüglich Ring-mit-1.

$E(\mathbb{Z}/\ n_1 \cdot n_2\mathbb{Z})$ *isomorph* $E(\mathbb{Z}/\ n_1\mathbb{Z}\ x\ \mathbb{Z}/\ n_2\mathbb{Z})$

Als Gruppe unter demselben Isomorphismus.

Vermutung:

$$E(\mathbb{Z}/\ n_1\mathbb{Z}\ \ x\ \ \mathbb{Z}/\ n_2\mathbb{Z}) \ = \ E(\mathbb{Z}/\ n_1\mathbb{Z})\ \ x\ \ E(\mathbb{Z}/\ n_2\mathbb{Z})$$

$$\varphi(n_1 \cdot n_2) \qquad\qquad \varphi(n_1) \qquad\quad \varphi(n_2)$$

$$(x\ ,\ \ y) \qquad\qquad (x\ , \qquad\quad y)$$

Beweis:

„=>": Es sei (x, y) Einheit.

Dann existieren (x', y') mit (x, y)(x', y') = (1, 1).

(x, y)(x', y') = (xx', yy').

„<=": Es seien x, y Einheiten.

Dann existieren x' und y' mit xx' = 1, yy' = 1.

Es folgt: (x, y)(x', y') = (1, 1)

Jetzt haben wir unsere Vermutung bewiesen, es fehlt aber immer noch eine exakte Formel für die Eulersche Phi-Funktion.

Ist $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ die Primzahlzerlegung von n in die verschiedenen Primzahlen $p_1 \cdot \ldots \cdot p_r$, $(\alpha \in \mathbb{N})$, so ist $\varphi(n) = \varphi(p_1^{\alpha_1}) \ldots \varphi(p_r^{\alpha_r})$.

Jetzt ist noch die Frage offen, wie man $\varphi(p^\alpha)$ für Primzahl p und $\alpha \in \mathbb{N}$.

$$E(\mathbb{Z}/\ p^\alpha\ \mathbb{Z}) \ = \ \{\overline{x}|\ \ x \in \mathbb{Z},\ (x, p)\ \textit{teilerfremd}\}\ .$$

$$\mathbb{Z}/\ p^\alpha\ \mathbb{Z} \ = \ E(\qquad)\ \ \textit{disjunkt vereinigt mit}\ \ \{\overline{x}|\ \ p|x\}\ .$$

Es gibt demnach p^α Elemente.

Es bleibt die Frage zu klären, welche Elemente x Vielfache von p sind und wieviele ich von diesen Elementen habe.

Um diese Frage zu beantworten, haben wir uns einen Zahlenstrahl vorgestellt, der mit dem „Nulltopf" beginnt und den „p-Topf" und seine Vielfachen aufweist.

Dabei kann man folgendes Beobachten:

$$\overline{p} \qquad \overline{pp} = \overline{p^2} \qquad \ldots \qquad p^{\alpha} = 0 \ .$$

Demnach gibt es $p^{\alpha - 1}$ Elemente, die durch p teilbar sind (= „Schlechten").

Uns interessiert aber die Zahl der „Guten", welche sich bestimmt zu

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha - 1} = p^{\alpha - 1} \cdot (p - 1) \ .$$

Mit diesem Ergebnis können wir unsere Formel für die Euler Phi-Funktion vervollständigen und halten folgendes fest:

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{\alpha_1}) \ldots \varphi(p_r^{\alpha_r}) \\ &= p_1^{\alpha_1 - 1} \cdot (p_1 - 1) \cdot \ldots \cdot p_r^{\alpha_r - 1} \cdot (p_r - 1) \end{aligned} \ .$$

Jetzt können wir abschließend an unserem obigen Beispiel überprüfen, ob und wie unsere Formel funktioniert:

n = 9: n = 3², p = 3, alpha = 2

$\varphi(9) = 3(3-1) = 6$

Ein Vergleich dieses Ergebnisses mit dem aus unserer Tabelle zeigt eine Übereinstimmung.

n = 4: n= 2², p = 2, alpha = 2

$\varphi(4) = 2(2-1) = 2$

Ein Vergleich mit der Tabelle liefert auch hier eine Übereinstimmung.

Somit haben wir eine Formel für die Eulersche Phi-Funktion gefunden, mit der auch die Einheitengruppe beschrieben werden kann.

Elementare Zahlentheorie WS 2003/04

Protokoll vom 04.11.03 (AE)

[Zurück zur Protokollübersicht]

Thema der Stunde: Eulers Zugang zur *Phi*-Funktion

Zu Beginn der Stunde stellte sich die Frage, wie Euler ohne den chinesischen Restesatz auf die *Phi*-Funktion kam. Zunächst definierten wir unser Ziel, eine explizite Formel für *Phi* zu finden. Um uns diesem Problem zu nähern, stellten wir die folgenden Fragen und begannen, Antworten zu suchen:

F1: Wie ist *Phi* definiert?

F2: Wozu ist *Phi* gut?

F3: Welche explizite Formel gibt es für *Phi*?

F4: Was wissen wir bereits über die Einheitengruppe von *Z/nZ?*

A1: *Phi* ordnet einer natürlichen Zahl *n* den Restklassenring *Z/nZ* zu, diesem wird die Einheitengruppe *E(Z/nZ)* zugeordnet und dieser Gruppe wiederum ihre Ordnung. Definitions- und Wertebereich sind also beides die natürlichen Zahlen.

A3: Wir wissen über *E(Z/nZ)*: Die Restklasse $\bar{a}$ ist genau dann Einheit von *Z/nZ*, wenn *(a, n)* teilerfremd sind (*a* Element von *Z*).

F5: Welche Elemente sind nicht teilerfremd? Wie viele?

A5: *N(n) :=* Anzahl der Elemente $\bar{a}$, für die gilt: *(a, n)* sind nicht teilerfremd, wobei *a* zwischen *0* und *n - 1* liegt.

Es gilt also folgendes: Anzahl von *E(Z/nZ) = N(n) + φ(n).*

Nun versuchten wir wiederum durch Fragen und Antworten *N(n)* zu bestimmen.

F6: Welche Elemente sind nicht teilerfremd?

F7: Was sind die Teiler von *n*?

F8: Wie lautet die Primfaktorzerlegung von *n*?

A8: $n = p_1^{\alpha 1} \ldots p_r^{\alpha r}$ mit Primzahlen p_i (*i* zwischen *1* und *r*).

A6: *(a, n)* nicht teilerfremd bedeutet: Es existiert p_i (*i* zwischen *1* und *r*) mit p_i teilt *a*.

F9: Wie viele *a* (*a* zwischen *0* und *n - 1*) werden von einer Primzahl *p* geteilt?

A9: Die Anzahl beträgt *n/p.*

Also gilt: $N(n) = n/p_1 + n/p_2 + \ldots + n/p_r - T_2$, wo T_2 := Anzahl der *a*, die durch mindestens *zwei* der p_i (*i* zwischen *1* und *r*) geteilt werden.

F10: Wie lässt sich T_2 durch Formeln ausdrücken?

A10: Definiere zunächst T_k := Anzahl der *a*, die durch mindestens *k* der p_i (*i* zwischen *1* und *r*) geteilt werden.

$T_2 = n/(p_1p_2) + n/(p_1p_3) + ... + n/(p_1p_r) + n/(p_2p_3) + ... + n/(p_{r-1}p_r) - T_3$

$T3 = n/(p_1p_2p_3) + ... - T_4$

...

$T_r = n/(p_1p_2 \cdots p_r)$

Also folgt:

$$N(n) = n/p_1 + n/p_2 + ... + n/p_r - n/(p_1p_2) + n/(p_1p_3) + ... + n/(p_1p_r) + n/(p_2p_3) + ... + (-1)^{r-1} n/(p_1p_2 \cdots p_r)$$

Schlussbemerkung: Wir haben die Formel für N(n) natürlich nicht sofort (wie oben dargestellt) herausgefunden, sondern zunächst falsche oder unzulängliche Formeln aufgestellt, diese teilweise an Beispielen überprüft und nach und nach verbessert.

Zurück
zur vorangehenden Stunde (31.10.03),
zur Protokollübersicht.

Protokoll zur Vorlesung Elementare Zahlentheorie vom 06.11.2003 (NB)

[Zurück zur Protokollübersicht]

I. Inhaltliches Denken

[Wiederholung der letzten Vorlesung]

$\varphi(n) = |E(\mathbf{Z}/n\mathbf{Z})| = n - T_1(n)$, mit $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ Primfaktorzerlegung.

$T_1(n) = (\sum^r_{i=1} n/p_i) - T_2(n)$

Wobei wir bedenken müssen, dass wir die Paare zählen: $|\{(p_i,x) \mid 0 \leq x \leq n-1, p_i \mid x\}|$. Hierbei tritt das Problem auf, dass ein gleiches x bei verschiedenen p_i vorkommen kann. Diese müssen wir also wieder abziehen:

$T_2(n) = (\sum_{i<j} n/(p_i \cdot p_j)) - T_3(n)$

...

$T_r(n) = n / (p_1 \cdot \ldots \cdot p_r)$

Also: $\varphi(n) = n - (\sum n/p_i) + (\sum n/(p_i \cdot p_j)) - \ldots (-1)^r n / (p_1 \cdot \ldots \cdot p_r)$.

II. Formales Denken (Formel umformen)

Wie sollen wir die Formel umformen?

- n ausklammern.
- Alles auf einen Nenner bringen.

Setze $q_i = 1 / p_i$ und erhalte: $\varphi(n) = n \cdot (1 - (\sum q_i) + (\sum q_i \cdot q_j) - \ldots (-1)^r q_1 \cdot \ldots \cdot q_r)$.

- Um weiter umformen zu können wählen wir Beispiele für ein kleines r und erhalten so einen Überblick.

Beispiele:

- $r = 1 : \varphi(n) = n \cdot (1 - q_1)$
- $r = 2 : \varphi(n) = n \cdot (1 - (q_1 + q_2) + q_1 \cdot q_2) = n \cdot (1 - q_1)(1 - q_2)$
- $r = 3 : \varphi(n) = n \cdot (1 - q_1 - q_2 - q_3 + q_1 \cdot q_2 + q_2 \cdot q_3 + q_1 \cdot q_3 - q_1 \cdot q_2 \cdot q_3 + q_1 \cdot q_2) = n \cdot (1 - q_1)(1 - q_2)(1 - q_3)$

Also:

$$\boxed{\varphi(n) = n \cdot (1 - 1/p_1) \cdot \ldots \cdot (1 - 1/p_r)}$$

Dies ist die sog. EULERsche-Phi-Funktion.

Probe:

$n = 12 = 2^2 \cdot 3^1$

$\varphi(12) = 12 \cdot (1 - 1/2) \cdot (1 - 1/3) = 12 \cdot 1/2 \cdot 2/3 = 4$

Nach Chinesischem Restesatz:
$\varphi(12) = \varphi(4) \cdot \varphi(3) = 2 \cdot 2 = 4$
Denn hier galt die Formel für tlfr. m_1 und m_2: $\varphi(m_1 \cdot m_2) = \varphi(m_1) \cdot \varphi(m_2)$. Diese Formel ist durch Termumformung in die Euler-Formel überführbar.

Vergleichen wir die beiden Methoden einmal:

- Chinesischer Restesatz: Hier wurde mittels der Gruppen- und Ringtheorie argumentiert. Der Beweis fand auf einer sehr abstrakten Ebene [DE 3 und 4] statt. Aber man erhält nicht nur eine Aussage über die Anzahl der Elemente der Einheiten, sondern wir bekommen Aussagen über die Struktur und die Isomorphietypen:
  $\boldsymbol{Z}/m_1m_2\boldsymbol{Z} \approx \boldsymbol{Z}/m_1\boldsymbol{Z} \times \boldsymbol{Z}/m_2\boldsymbol{Z}$ (als Ring-m-1) bzw. $E(\boldsymbol{Z}/m_1m_2\boldsymbol{Z}) \approx E(\boldsymbol{Z}/m_1\boldsymbol{Z}) \times E(\boldsymbol{Z}/m_2\boldsymbol{Z})$ (als Gruppen) für m_1, m_2 tlfr.

  Allgemein: $E(\boldsymbol{Z}/n\boldsymbol{Z}) \approx E(\boldsymbol{Z}/p_1^{\alpha 1} \cdot \boldsymbol{Z}) \times \ldots \times E(\boldsymbol{Z}/p_r^{\alpha r} \cdot \boldsymbol{Z})$, wenn $n = p_1^{\alpha 1} \cdot \ldots \cdot p_r^{\alpha r}$.

  Also gilt nach der Formel: $\varphi(n) = \varphi(p_1^{\alpha 1}) \cdot \ldots \cdot \varphi(p_r^{\alpha r})$ mit $\varphi(p^\alpha) = p^\alpha - p^{\alpha - 1} = p^{\alpha - 1}(p-1) = p^\alpha(1-1/p)$. [Dies ergibt eingesetzt genau die Euler-Formel!]
- Euler: Hier kommt man mit ganz elementaren Rechnungen aus und die Gruppen- und Ringtheorie wird nicht benötigt. Man bekommt allerdings auch nur die Anzahl der Elemente. Weitere (Struktur-)Aussagen lassen sich nicht gewinnen.

III. Weiterführendes Denken (Fragen und Planen)

Wir interessieren uns ja für die Einheitengruppe $E := E(\boldsymbol{Z}/n\boldsymbol{Z})$. Bis jetzt haben wir: $\varphi(n)=|E(\boldsymbol{Z}/n\boldsymbol{Z})|$.

Also stellen wir weitere Fragen an die Gruppe: **[FRAGEN]**

1. Welche Untergruppen gibt es?
2. Welche Elemente sind in der Gruppe? Was sind die Elementordnungen?
3. Was sind die Normalteiler und was ist das Zentrum?
4. Gibt es ein minimales Erzeugendensystem? Ist E zyklisch?
5. Was sind die Isomorphietypen von $E(\boldsymbol{Z}/p^\alpha\boldsymbol{Z})$?

[Konvention: Ich schreibe $\underline{x}$ für die Restklassen von x.]

Finden der Antworten: **[PLANEN]**

Zu 2.:
Die Elemente: $E=\{\underline{x} \mid 0 \leq x \leq n-1, ggT(x,n)=1\}$
Die Elementordnungen: $|\langle\underline{x}\rangle| = o(\underline{x}) = Min\ \{ k \text{ aus } \boldsymbol{N} \mid \underline{x}^k = \underline{1}\} =: m$
Beh.: m teilt diese k aus $\boldsymbol{N}$.
Beweis: Division mit Rest: $k = m \cdot q + r\ (0 \leq r < m)$, $\underline{1} = \underline{x}^k = \underline{x}^{mq+r} = (\underline{x}^m)^q \cdot \underline{x}^r = \underline{x}^r$, Da aber m minimal ist, ist $r = 0$.

Zu 3.:
Diese Frage ist unerheblich, da E eine abelsche Gruppe ist und somit jede Untergruppe Normalteiler ist.

Zu 4.:
Zuerst betrachten wir allgemeine zyklische Gruppen:
Analyse:

- Gruppe bezgl. der Multiplikation: $<.a> = \{a^0=1, a^1, ..., a^{m-1}\}: m$
- Gruppe bezgl. der Addition: $<.b> = \{ 0b, 1b, ..., (m-1)b\} \approx \boldsymbol{Z}/m\boldsymbol{Z} = \{\underline{0}, \underline{1}, ..., \underline{m-1}\} = <\underline{1}>$, wobei hier $b \leftrightarrow \underline{1}$ bijektiv abgebildet wird.
- Unendl. zykl. Gruppe: $<.a> = \{..., a^{-2}, a^{-1}, a^0, a^1, ...\} \approx \boldsymbol{Z}/0\boldsymbol{Z} \approx \boldsymbol{Z} = \{..., -2, -1, 0, 1, 2, ...\} = <1>$ wobei hier $a \leftrightarrow 1$ bijektiv abgebildet wird.

Also sind alle zyklischen Gruppen isomorph zu $\boldsymbol{Z}/m\boldsymbol{Z}$.

Ist nun auch $E(\boldsymbol{Z}/n\boldsymbol{Z})$ zyklisch?

Betrachten wir in Gruppenarbeit Beispiele. Zuvor aber noch ein hilfreicher Satz:
Beh.: $|U|$ teil $|G|$ für U Untergruppe der Gruppe G.
Beweis: $G = U$ *vereinigt mit* Ug_1 *vereinigt mit* Ug_2 *vereinigt mit ... vereinigt mit* Ug_r . Da alle Nebenklassen gleich viele Elemente enthalten, gilt natürlich: $|G| = r \cdot |U|$, q. e. d.

Gehen wir nun die Beispiele an:

m	**25**	**13**	**11**	**7**	**5**	**27**	**9**	**3**	**16**	**8**	**4**	**2**
|E|	20	12	10	6	4	18	6	2	8	4	2	1

Wir müssen also jeweils testen, ob die Ordnung s von $\underline{x}$ aus $E(\boldsymbol{Z}/n\boldsymbol{Z})$ gerade gleich $|E|$ ist. Für diese n ist $E(\boldsymbol{Z}/n\boldsymbol{Z})$ zyklisch.
Die weitere Untersuchung findet in der nächsten Vorlesung statt.

Zurück
zur vorangehenden Stunde (04.11.03),
zur Protokollübersicht.

Elementare Zahlentheorie WS 03/04
Protokoll vom Fr., 07.11.03.

[Zurück zur Protokollübersicht]
[Dieses Protokoll muss noch redigiert werden.]

Besprechung der Hausaufgaben:

F1: Wie kann man mit den Restklassen eine Probe machen?

Beispiel:

Rechnung: 13765128+ 2831761= 16597889

$(13765128)_9 = 6$ und $(2831761)_9 = 1$.
Da es sich bei den Restklassen um einen **Ring-m-1** handelt müsste also
$(13765128+ 2831761)_9 = (6+1)_9 = 7$ sein.

Probe: $(16597889)_9 = 8 \neq 7$. Also ist unser Ergebnis falsch.

Besprechung der **Hausaufgabe 4**:

a) Jede zyklische Gruppe ist isomorph zu einer Faktorgruppe der Gruppe **Z** aller ganzen Zahlen.

Sei $c_n = \{c^k / k \epsilon \mathbf{Z}\}$ **multiplikativ.** Außerdem: $c_n = \langle c \rangle$. und $|c_n| = n$

F2. Wie bekommt man einen Isomorphismus?
A1. Nach Homomorphiesatz.
F3. Welcher Homomorphismus? Sei $\varphi: (k \rightarrow c^k) : \mathbf{Z} \rightarrow c_n$.
F4. Ist φ ein Homomorphismus?
Es seien $i,j \epsilon \mathbf{Z}$. $(i+j)\varphi = c^{i+j} = c^i * c^j = i\varphi * j\varphi$.
A3. Also ist φ ein Homomorphismus.
F5. Warum gilt Homomorphie obwohl aus dem "+" ein "*" wurde?
A3. Eine Abbildung φ ist homomorph, wenn folgendes gilt: $(x *_1 y)\varphi = x\varphi *_2 y\varphi$,
mit $x, y \epsilon (G,*_1)$ und $x\varphi, y\varphi \epsilon (H,*_2)$ **(I)**.
F6. Warum reicht **(I)** schon aus um die Homomorphie zu zeigen, ohne zu beweisen, dass das neutrale Elemente auf das neutrale Element**(III)** und das inverse Element auf das Inverse**(II)** abgebildet wird?
Es gilt: $0\varphi = (0+0)\varphi$. Daraus folgt: $1 = 0\varphi * (0\varphi)^{-1} = 0\varphi * (0\varphi * (0\varphi)^{-1}) = 0\varphi$
Also folgt **(III)** aus **(I).**
Außerdem gilt: $i + (-i) = 0$. Also ist $(i + (-i))\varphi = 0\varphi = 1$. Daraus folgt: $i\varphi * (-i)\varphi = 1$
Und somit: $(i\varphi)^{-1} * i\varphi * (-i)\varphi = (i\varphi)^{-1}$. Also $\mathbf{(-i)\varphi = (i\varphi)^{-1}}$. Also folgt auch **(II)** aus **(I).**
A4. Also ist φ ein Homomorphismus und **(II), (III)** folgen aus **(I).**
F7. Was ist der **Kern** von φ?
Wir wissen: $c^k \neq 1$ für alle $k \epsilon \{1,\ldots,n-1\}$, und $\langle c \rangle = \{c^0, c^1,\ldots,c^{n-1}\}$, mit $c^n = 1$.
Und Kern $\varphi = \{z \epsilon \mathbf{Z} / z\varphi = 1\}$. Beh.: Kern $\varphi = \{n*z / z \epsilon \mathbf{Z}\} = n* \mathbf{Z}$.
Beweis: 1. $n* \mathbf{Z}$ ist Teilmenge vom Kern φ: $\varphi = c^{n*k} = (c^n)^k = 1^k = 1$
2. Der Kern von φ ist Teilmenge von $n* \mathbf{Z}$: Der Beweis funktioniert mittels der Division mit Rest. Hier kann wie in der vorangegangenen Vorlesung ein Widerspruch zur Minimalität von n bewiesen werden.

A5. Also ist der Kern φ= n* **Z**.
F8. Was ist das **Bild** von φ?
A6. Wegen k→ c^k für kϵ{0, 1,…, n-1} gilt: **Bild φ= c_n.**
Nach Homomorphiesatz folgt: **Z** /n* **Z** entspricht c_n unter dem Isomorphismus:
φ˜: = (z˜ → zφ): **Z**/ n* **Z** → c_n.

b) Die Untergruppen von **Z** haben die Form n**Z**= {nk/ k in **Z**}
G: = **Z zyklisch**, mit G= <1> **additiv**, und U≤ G.
1*mϵ U, mϵ **N**, m= min {k/ 1*kϵ U, kϵ **N**}
1. Fall: U= {0}= 0* **Z**.
2. Fall: U≠ {0}:
a) U≤ <m>. Beweis: U (ϵU)= mq (ϵU) + r (ϵU) für alle r größer 0 und kleiner gleich m.
Daraus folgt: r = 0, und daraus folgt U≤ <m>= {mk/ kϵ**Z**}= m**Z**.
b) aus mϵ U folgt automatisch mkϵ U.

c) Die Untergruppen von **Z**/ n**Z** haben die Form U/ n**Z** für eine Untergruppe n**Z**/ ≤ U ≤ **Z**, mit U= m**Z** für einen Teiler mϵ $\mathbf{N_0}$ von n.
Es sei X≤ **Z**/ n**Z**. (z.z.: X= U/ n**Z** für eine Untergruppe U kleiner **Z** mit n**Z**≤ U)
F9. Welches U kann man nehmen?
A7. U: = {zϵ **Z**/ zφϵ X}= $X\varphi^{-1}$.

Zurück
zur vorangehenden Stunde (06.11.03),
zur Protokollübersicht.

Elementare Zahlentheorie WS 2003/04

11.11.2003 AZ

[Zurück zur Protokollübersicht]

Z/n **Z** ist ein R-m-1.

1) Additive Struktur: **Z**/n**Z** zyklische Gruppe.

2) Multiplikative Struktur: E(**Z**/n**Z**) ist eine Gruppe mit φ(n) Elementen.

Thema: Struktur der "primen Restklassengruppe" [(Prime Restklassen)-Gruppe]

Kann man 2) in zyklische Gruppen zerlegen?

Frage: Ist E(**Z**/n**Z**) zyklisch? (Zyklisch: Ordnung o($\bar{a}$) vom Erzeuger *a* der zyklischen Gruppe muss gleich φ(*n*) sein.)

[Ab hier muss noch redigiert werden.]

Frage: $|\langle\bar{a}\rangle|$ für a ϵ E(**Z**/n**Z**) = o($\bar{a}$) = Min{m ϵ N| $a^m = 1$}

Beispiele:

bekannt: $|\langle\bar{a}\rangle|$ teilt |E(**Z**/n**Z**)|

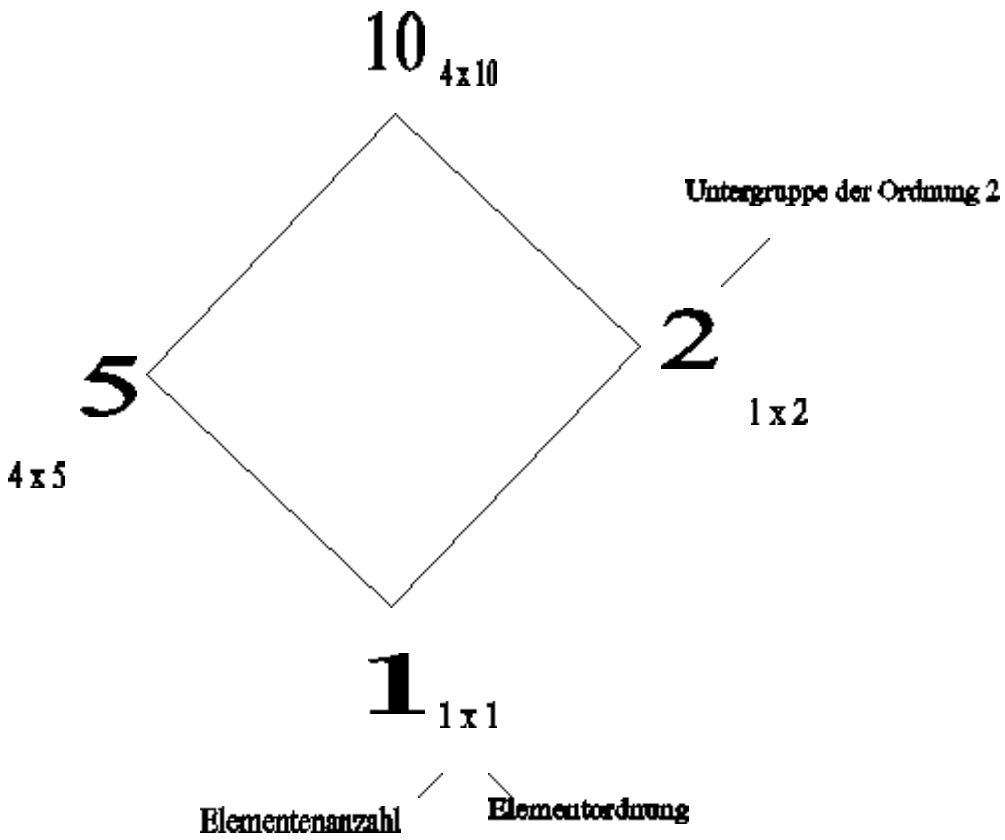
o($\bar{a}$) teilt φ(n) , also sind die Kandidaten für o($\bar{a}$) die Teiler von φ(n)

n	φ(n)	alle Elemente von E & o($\bar{a}$)	E zyklisch?
4	2	$\overline{\{1,3\}}$: $\overline{1,2}$	Ja, E ≡ C_2
8	4	$\overline{\{1,3,5,7\}}$: $\overline{1,2,2,2}$	Nein
16	8	$\overline{\{1,3,5,7,9,11,13,15\}}$: $\overline{1,4,4,2,2,4,4,2}$	Nein
6	2	$\overline{\{1,5\}}$: $\overline{1,2}$	Ja, E ≡ C_2
3	2	$\overline{\{1,2\}}$: $\overline{1,2}$	Ja, E ≡ C_2
5	4	$\overline{\{1,2,3,4\}}$: $\overline{1,4,4,2}$	Ja, E ≡ C_4 , E=$\langle\bar{2}\rangle$=$\langle\bar{3}\rangle$

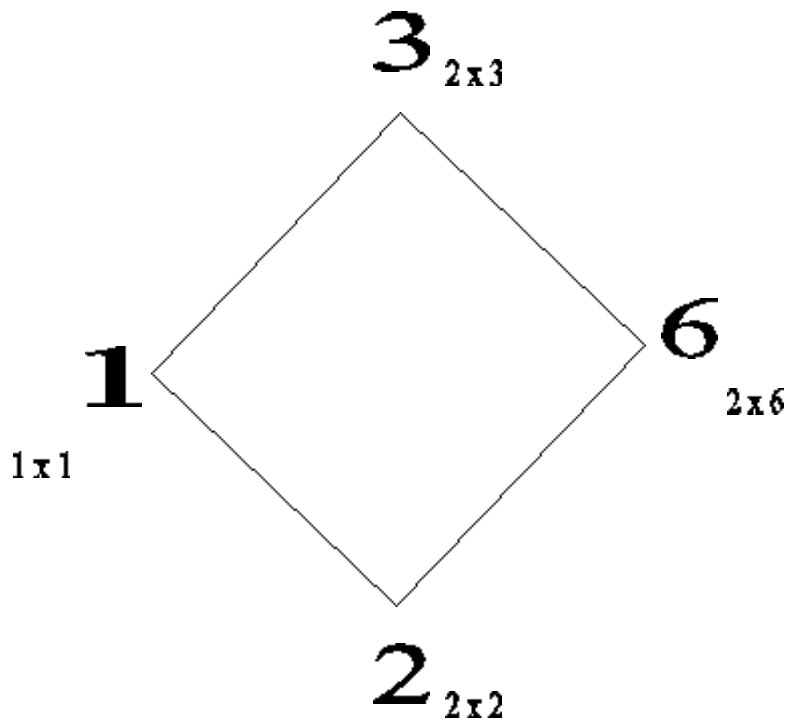
7	6	$\overline{\{1,2,3,4,5,6\}} : \overline{1,3,6,3,6,2}$	Ja, $E \equiv C_6$, $E=<\bar{3}>=<\bar{5}>$, $\bar{3}=\bar{5}^{-1}$
11	10	$\overline{\{1,2,3,4,5,6,7,8,9,10\}}$: $\overline{1,10,5,...}$	Ja, $E \equiv C_{10}$
3^2	6	$\overline{\{1,2,4,5,7,8\}} : \overline{1,6,3,6,3,2}$	Ja, $E \equiv C_6$

Elemente der Untergruppen

Beispiel: Elemente der zyklischen Gruppe mit φ(n)=10



Beispiel: Elemente der zyklischen Gruppe mit φ(n)=6



Was sehen wir jetzt, was schließen wir aus den Beispielen?

1. Vermutung: E(**Z**/p**Z**) ist zyklisch (multiplikative Gruppe des Körpers (**Z**/p**Z**))

2. Vermutung: E(**Z**/2^e**Z**) ist nicht zyklisch, denn E(**Z**/2^e**Z**) = $<\bar{5}>$* $<\text{-}\bar{1}>\equiv C_2 e\text{-}2 \text{ x } C_2$

Dazu:

Beispiel 1: n=8, φ(n)= 4

Es gibt drei Untergruppen der Ordnung 2. Daher kann man immer 2 dieser Untergruppen auswählen, um ganz E zu erzeugen. Wähle also zum Beispiel E= $<\bar{3}>$ * $<\bar{5}>$. Dabei erzeugt dieses innere direkte Produkt die Menge {1,3,5,7} mit 3*5 = 7

Beispiel 2: n = 16, φ(n)=8

Hier ist E = C_4 x C_2 = $<\bar{3}>$ * $<\overline{15}>$ = $<\bar{3}>$ * $<\overline{\text{-}1}>$ = $<\bar{5}>$ * $<\overline{15}>$

Man kann auch hier immer zwei Untergruppen beliebig auswählen, um E zu erzeugen.

Beispiel 3: n = 32, φ(n) = 16

$E = C_8 \times C_2 = \langle \bar{5} \rangle * \langle \bar{-1} \rangle$

Ingesamt folgt also, dass $E(\mathbf{Z}/2^e\mathbf{Z})$ nicht zyklisch ist, denn $E(\mathbf{Z}/2^e\mathbf{Z}) = \langle \bar{5} \rangle * \langle \bar{-1} \rangle \equiv C_2 e\text{-}2 \times C_2$

Zusatz: Bei ungeraden Primzahlen entfällt die <-1> und es folgt, dass E dann zyklisch ist.

Beweis der ersten Vermutung

[Existieren Elemente der Ordnung p-1? Beh.: $E(\mathbf{Z}/p\mathbf{Z}) = C_{p-1}$. In C_{p-1} gibt es zu jedem Teiler k von p-1 genau eine Untergruppe der Ordnung k, also hat C_{p-1} höchstens k Elemente der Ordnung k.]

$E(k) := \{\bar{x} \in E \mid o(\bar{x}) \text{ teilt } k\} : \bar{x}^k = 1, \bar{x}^k - 1 = 0$; dh, $\bar{x}$ ist Nullstelle von $X^k - 1 \in K[X]$ mit $K[X] = \mathbf{Z}/p\mathbf{Z}$

Also ist $| E(k) | \leq k$. Warum?

$p(X) = (X\text{-}x_1)...(X\text{-}x_r)$ $q(X) = ? = (X\text{-}x_{1'})...(X\text{-}x_{s'})$

Angenommen, $p(X) = (X\text{-}x_1)p_2(X)$

x_2 ist Nullstelle von p, daraus folgt dann, dass x_2 Nullstelle von p_2 ist.

Dann folgt mit Division mit Rest für Polynome über Körper, dass $(X\text{-}x_2) \mid p_{2(}X)$.

Also sind die Nullstellen eindeutig bestimmt.

Elementare Zahlentheorie WS 2003/04

Protokoll der Sitzung vom 13.11. (SM)

[Zurück zur Protokollübersicht]

Fragen: Ist $E = E(\mathbf{Z} / n\mathbf{Z})$ zyklisch?
Vermutungen:

1. Aus $n = p$ Primzahl folgt: E ist zyklisch.
2. Aus $n = 2^4$ folgt $E = <5> * <-1>$.
3. Aus $n = p^k$, $2 \neq p$ folgt...

Planen. Zu 1)
Satz: G sei eine endliche Gruppe, $|G| =: m$.
Für $k \in \mathbf{N}$ setze $G(k) := |\{x \in G \mid x^k = 1\}| = |\{x \in G \mid o(x) \mid k\}|$.

Dann sind äquivalent:
(1) G ist zyklisch.
(2) $G(k) \leq k$ für alle $k \in \mathbf{N}$.

[Ab hier muss noch redigiert werden.]

Beweis: Aus (1) folgt (2).

Aus (2) folgt (1).

Schreiben zu 1) Beweis:

Schritt 1: $E(k) \leq k$ für alle k.
Schritt 2: Nach Satz [(2)=>(1)], ist E zyklisch.||

Beispiel:

R := $\mathbf{Z} / 2\mathbf{Z} * \mathbf{Z} / 2\mathbf{Z}$ = {(0, 0); (0, 1); (1, 0); (1, 1)}
$X(X - (1, 1)) = X^2 - X \in R[X]$
$(1, 0)^2 - (1, 0) = (0, 0)$
$(0, 1)^2 - (0, 1) = (0, 0)$
$(1, 1)^2 - (1, 1) = (0, 0)$
$(0, 0)^2 - (0, 0) = (0, 0)$

$(x - (1, 0))\,(x - (0, 1)) = x^2 - x+0$
$x^2-x = (x -(0, 0))(x - (1, 1)) = (x - (1, 0))\,(x -(0, 1))$

Zu zeigen:

Aus (2) folgt (1) :
$G[k] = |\ \{e \in G \mid o(x) = k\}\ |$

G ist zyklisch, d.h. $G = \mathbf{Z} / m\mathbf{Z} = H$, H ist zyklisch $H(k) \leq k$
$H(k) = k \leq G(k) \leq G[k]$, $| H | = m = | G |$
für $k \mid m$
$G = \mathrm{U}_{k \mid m} G'[k]$
$| G | = \mathrm{S}_{k \mid m} G[k]$
ist gleich der Menge $\{x \in G \mid o(x) = k\}$
$\mathrm{H} = \mathrm{U}_{\mathrm{k} \mid \mathrm{m}} H'[k]$
$| H | = \mathrm{S}_{\mathrm{k}\mid\mathrm{m}} \mathrm{H}[\mathrm{k}]$.
[Gilt $H[k] \geq G[k]$ für alle $k \mid m$? Denn dann $H[k] = g[k]$ für alle $k \mid m$, also insbesondere $H[m] = G[m]$, G zyklisch. ||
$\neq 0$, etwa $o(g) = m = | < g > | = | G |, = G$.]

Noch zu zeigen: $H[k] \geq G[k]$ für alle $k \mid m$.

1.Fall: $G[k] = 0$. *ok* $H[k] > 0$
2.Fall: Es existiert $y \in G$ mit $o(y) = k$: mit $k \geq G(k)$ und $(k) = k$
also $G(k) = k$ und $G[k] = H[k]$.

Def.: $n \in \mathbf{Z}$, $m \in \mathbf{Z}$ heißt Primitivwurzel mod n, wenn $E(\mathbf{Z} / n\mathbf{Z})$ zyklisch ist [mit $Q(n)$ Elementen] und $<m> = E(\mathbf{Z} / n\mathbf{Z})$ und gilt [$o(\mathrm{m}) = \varphi(n)$].

Liste der kleinsten positiven Primitivwurzeln mod p für die P_2 p <100:

0 < m, $E(\mathbf{Z} / p\mathbf{Z}) = C_{p-1}$	$\varphi(p) = p - 1$
1	2
2	3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 76, 83
3	7, 17, 31, 43, 79, 89
5	23, 47, 73, 97
6	41
7	71

Schreiben zu 2)
Sei $n = 2^{ä}$ mit $a > 3$ $q(2^{ä}) = 2^{ä-1} = E(\mathbf{Z} / 2^{ä}\mathbf{Z})$.

1. Vermutung
$a^{2^{a-1}} = 1$ für alle $a \in E = E(\mathbf{Z}/2^{a}\mathbf{Z})$.

Beweis:

i) $a = 3 : E = E(\mathbf{Z} / 8\mathbf{Z}) = \{1,3,5,7\} = C_2 x C_2$.

Zu zeigen $a^2 = 1$ für $a \in E$
$q = 4 : E(\mathbf{Z} / 16\mathbf{Z}) = <5> * <-1>$.
Zu zeigen $5^4 = 1$!
$x^1 = 1$ in $(\mathbf{Z}/2^{a}\mathbf{Z})$ bedeutet:
$x^1 \equiv 1 \bmod 2^{a}$, $x^{1-1} \equiv 0$, $a^a \mid x^1 - 1$.

ii) Vollständige Induktion nach a

Induktionsschritt:
Es sei $a > 3$.
Es gelte $x^{2^{a-2}} \equiv 1 \bmod 2^a$ für alle $x \in E(\mathbf{Z}/2^a\mathbf{Z})$ d.h. für alle $x \in \mathbf{Z}$ mit $2 + x$.
[Zu zeigen $x^{2^{a-1}} \equiv 1 \bmod 2^{a+1}$ für alle $2 \dagger x \in$ Z.]
Es folgt:
$x^{2^{a-2}} = 1 + 2^a * d$ für ein $d \in \mathbf{Z}$,
$x^{2^{a-1}} = x^{a^{a-2} * 2} = (x^{2^{a-2}})^2 = (1 + 2^a d)^2$
$= 1 + 2^{a-1} d + (2^a d)^2 \equiv 1 \bmod 2^{a+1}$. ||

Zur vorangehenden Stunde (11.11.03),
zur nächsten Stunde (18.11.03),
zur Protokollübersicht.

Elementare Zahlentheorie

Stundenprotokoll vom 18.11.2003 (MH)

[Zurück zur Protokollübersicht]
[Dieses Protokoll muss noch redigiert werden.]

Die Vorlesung beginnt mit einer kurzen Zusammenfassung der Themen aus den letzten Vorlesungen.

Dabei kommt die Frage auf, wie wir uns dabei fühlen, wenn wir über Einheitengruppen und Ähnliches sprechen. Diese Frage wird anscheinend mehrheitlich mit einer negativen Empfindung verbunden, was hauptsächlich dadurch zu begründen war, dass uns der Realitätsbezug und der Sinn unserer vorangegangenen Überlegungen fehlt.

Es stellt sich uns die Frage, warum wir das überhaupt wissen wollen. Warum machen wir das?

Diese Frage stellt sich auch häufig im Mathematikunterricht, wodurch wir eine Überleitung zur Schulsituation geschaffen haben. Wir stellen fest, dass die Schüler den Lehrer oft fragen, warum sie beispielsweise das Addieren lernen müssen, wo es doch Taschenrechner gibt. Den Schülern fehlt die Motivation – der Bezug zur Realität. Als Lehrer ist es jedoch unsere Aufgabe, die Schüler jeden Tag erneut zu motivieren. Es stellt sich also die Frage, ob die meisten Menschen in ihrem späteren Berufsleben überhaupt die Mathematik benötigen. Unsere Antwort auf diese Frage ist ein eindeutiges Ja, denn in allen Wissenschaften, beispielsweise der Chemie oder Biologie, aber auch in der Architektur oder im Rechtswesen wird die Mathematik ständig benötigt. Sei es um Statistiken zu erstellen oder zu lesen, Streitfragen zu klären, Populationen mithilfe des Räuber-Beute-Systems zu errechnen, oder sei es nur die Methodik, die das Fach Mathematik vermittelt.

Oft jedoch betreibt man Mathematik auch, weil es einfach nur „schön“ ist. Womit wir wieder zurück in der Universität, in unserer Vorlesung angekommen wären. Wir betreiben Mathematik also einfach momentan nur, weil sie schön ist. Bei uns ist der Satz, den wir gerade zu entwickeln versuchen, schön.

Zahlentheorie als solche ist ein Bereich der Mathematik, in dem es nur sehr wenige Anwendungen gibt und den man betreibt, weil es einem Spaß macht. Als ein Beispiel für eine Anwendung der Zahlentheorie werden letztendlich doch noch die Kryptosysteme (Verschlüsselung) gefunden. Mithilfe der Zahlentheorie können Nachrichten verschlüsselt werden (auch öffentlich), die von keinem Anderen als dem Empfänger entschlüsselt werden können.

Wir betreiben aber im Moment Mathematik und Zahlentheorie deshalb, weil es Spaß macht und weil die Methoden, die zur Lösung führen, schön sind.

Nach dieser kleinen Exkursion kehren wir zu unserem Stoff zurück.

Wir wollen einen Satz aufstellen:

$$E = (\mathbb{Z} \mid 2^{\alpha}\mathbb{Z}) = \langle 5 \rangle \circ \langle -1 \rangle \quad : 2^{\alpha-1} \quad .$$

1. Vermutung:

$a^{2^{\alpha-2}} = 1, \qquad \text{für alle } a \in E$ (schon gezeigt).

$5^{2^{\alpha-2}} = 1, \qquad \text{in } \mathbb{Z} \mid 2^{\alpha}\mathbb{Z}$, (Beispiel: $\alpha = 3: 5^2 = 1$).

2. Vermutung:

$$o(5) = 2^{\alpha-2}, \text{ also } 5^{2^{\alpha-3}} \neq 1, \text{ in } \mathbb{Z}|2^{\alpha}\mathbb{Z} \qquad \text{für alle } \alpha \geq 3 \cdot$$

Planung des weiteren Vorgehens:

- *Frage*: Was ist noch zu zeigen?

- *Antwort*: Die zweite Vermutung

- *Plan*: Beweis per vollständiger Induktion

Wir beschließen also, die zweite Vermutung mithilfe von **Vollständiger Induktion** zu beweisen.

Induktionsverankerung:

$$\alpha = 3: 5^{2^{3-3}} = 5^1 = 5 \neq 1, \text{ in } \mathbb{Z}|8\mathbb{Z} \cdot$$

Induktionsannahme:

$$\text{Es sei } 5^{2^{\alpha-3}} \neq 1, \quad \text{für ein } \alpha \geq 3 \quad \text{in } \mathbb{Z}|2^{\alpha}\mathbb{Z}, \quad \text{d.h.}$$
$$x := (5^{2^{\alpha-3}} - 1) \neq 0 \mod 2^{\alpha} \cdot$$

Induktionsschritt:

$$\alpha \rightarrow (\alpha+1) \ .$$

Zu zeigen:

$$\tilde{5}^{2^{(\alpha+1)-3}} \neq \tilde{1} \qquad \text{in } \mathbb{Z}|2^{(\alpha+1)}\mathbb{Z} \cdot$$

Zwischenfrage:

Wir stellen fest, dass wir ein Problem haben. Wie bekommen wir also die Schwierigkeit in den Griff, dass wir uns in verschiedenen Restklassen befinden?

Um diese Frage zu beantworten, beschließen wir, uns erst einmal eine konkrete Vorstellung zu machen.

--> Topfrechnen.

Wir untersuchen, wie die Töpfe „Schlange“ und „Quer“ aussehen.

Wir stellen folgendes fest:

$$1 = 1 + 2^{\alpha}\mathbb{Z}$$
$$2^{\alpha}-1 = 2^{\alpha}-1 + 2^{\alpha}\mathbb{Z}$$

$$\tilde{1} = 1 + 2^{\alpha+1}\mathbb{Z}$$
$$2^{\alpha+1}-1 = 2^{\alpha+1}-1 + 2^{\alpha+1}\mathbb{Z}$$

Beim Vergleich der beiden Topfmengen können wir feststellen, dass der „Quer“-Topf doppelt so viele Elemente besitzt, wie der „Schlange“-Topf.

Zudem sind die Elemente des „Schlange“-Topfes im zugehörigen „Quer“-Topf enthalten.

Es lässt sich feststellen, dass jeder „Quer“-Topf in zwei „Schlange“-Töpfe zerfällt:

$$1 = \tilde{1} \cup (1 \tilde{+} 2^{\alpha})$$
$$0 = \tilde{0} \cup (0 \tilde{+} 2^{\alpha})$$
$$\dots$$

$$2^{\alpha}\mathbb{Z} = 0$$
$$2^{\alpha+1}\mathbb{Z} = 2\cdot 2^{\alpha}\mathbb{Z} = \tilde{0}$$

, woraus sich ergibt, dass $2^{\alpha}\mathbb{Z}$ größer ist.

Jetzt wissen wir etwas mehr über die Struktur der Töpfe. Es ist üblich nicht mehr mit „Töpfen“ zu rechnen, sondern stattdessen Repräsentanten zu wählen.

Nun können wir mit der **Vollständigen Induktion** fortfahren.

Wir haben:

$$x := (5^{2^{\alpha-3}} - 1), \qquad x + 1 = 5^{2^{\alpha-3}}$$

Uns interessiert aber:

$$5^{2^{\alpha-2}} = (x+1)^2 \text{ , bzw.}$$

$$y := (5^{2^{\alpha-2}} - 1) = (x+1)^2 - 1 = x^2 + 2 \cdot x \,.$$

Wir wollen zeigen, dass

$$2^{\alpha+1} \nmid y, \quad d.h. \quad 5^{2^{\alpha-2}} - 1 \neq 0 \mod 2^{(\alpha+1)} \,.$$

Wir wissen aber bereits:

$$2^{\alpha} \nmid x \qquad \text{und somit} \qquad 2^{\alpha+1} \nmid 2 \cdot x \,.$$

Da sich y aus einer Summe zusammensetzt, deren zweiter Summand bereits nicht von $2^{\alpha+1}$ geteilt wird, sollte nachgewiesen werden, dass der erste Summand geteilt wird von diesem Faktor, um sicher zu stellen, dass die gesamte Summe, somit also y, nicht von $2^{\alpha+1}$ geteilt wird.

Wenn dies gezeigt ist, haben wir per Vollständiger Induktion die zweite Vermutung gezeigt.

Die letzte Überprüfung wird nach einigen verzweifelten Ansätzen auf die nächste Vorlesung verschoben.

Zum Seitenanfang,
zur vorangehenden Stunde (13.11.03),
zur Protokollübersicht,
zur nächsten Stunde (20.11.03).

Elementare Zahlentheorie WS 2003/04

Protokoll vom 20.11.03 (AE)

[Zurück zur Protokollübersicht]

Themen der Stunde:

1) Die Einheitengruppe $E(Z/2^aZ)$ für $a > 2$

2) Prüfcodes

Zu 1):

Es sei $E := E(Z/2^aZ)$ für $a > 2$.

Behauptung: E ist als inneres direktes Produkt mit den zyklischen Faktoren

$< \bar{}5 >$ und $< \bar{}3 >$ darstellbar. ($|E| = |2^{a-1}|$)

1. Vermutung: $(\bar{}a)^{(2)\wedge(a-2)} = \bar{}1$ für alle $\bar{}a$ aus E.

2. Vermutung: $o(\bar{}5) = 2^{a-2}$

Zu zeigen: $(\bar{}5)^{(2)\wedge(a-3)}$ ist nicht gleich $\bar{}1$ in $Z/2^aZ$ $(a > 2)$

Induktionsvorrausetzung: $(\bar{}5)^{(2)\wedge(a-3)}$ ist nicht gleich $\bar{}1$ in $Z/2^aZ$ $(a > 2)$,

das heißt $x := (\bar{}5)^{(2)\wedge(a-3)} - 1$ ist nicht aus 2^aZ.

Zu zeigen: $(\sim 5)^{(2)\wedge(a-2)}$ ist nicht gleich ~ 1 in $Z/2^{(a+1)}Z$, das heißt $y := (\bar{}5)^{(2)\wedge(a-2)} - 1$ ist nicht aus $2^{a+1}Z$.

Nach der 1.) Vermutung gilt: $(5)^{(2)\wedge(a-1)}$ ist aus 2^xZ und $(5)^{(2)\wedge((a-1)-2)} - 1$ ist aus $2^{a-1}Z$.

Zu zeigen: y ist nicht aus $2^{a+1}Z$, das heißt 2^{a+1} teilt nicht y.

Betrachte: $y = x^2 + 2x$; 2^a teilt nicht x; 2^{a+1} teilt nicht $2x$.

Zu Zeigen: 2^{a+1} teilt x^2

Wir wissen: 2^{a-1} teilt nicht x, also: $(2^{a-1})\wedge 2 = 2^{(a-1)2}$ teilt x^2 . Es gilt: $2a - 2 = a + (a - 2)$ und $a - 2 > 0$, da $a > 2$.

Es folgt: 2^{a+1} teilt x^2 und 2^{a+1} teilt nicht $2x$. Damit folgt: 2^{a+1} teilt nicht y.

Es bleibt noch zu zeigen, dass $< \bar{}5 >$ und $< \bar{}3 >$ ein inneres direktes Produkt bilden.

3. Vermutung: $-\bar{}1$ *ist nicht aus* $< \bar{}5 >$ in $E(Z/2^aZ)$.

Beweis: Es gilt: 5 ist kongruent 1 modulo 4. Daraus folgt: 5^r *ist kongruent* 1 modulo 4 für jede natürliche Zahl r. Daraus folgt 1 ist nicht kongruent (-1) modulo 4

und 5^r ist nicht kongruent (-1) modulo 4. Daraus folgt: 5^r ist nicht kongruent zu -1 modulo 2^a.

Es folgt also: $(-\bar{}1)$ ist nicht aus $< \bar{}5 >$ in $E\ (Z/2^aZ)$

Also ist E vom Isomorphietyp: $C_{2\ \wedge\ (a-2)} * C_2$ (* steht hier für das kartesische Produkt bzw. äußere Produkt)

Fazit:

Die Einheitengruppe von $Z/2^aZ$ ist inneres direktes Produkt der zyklischen

Faktoren $< \bar{}5 >$ und $< \bar{}3 >$. Damit haben wir die Struktur der Gruppe analysiert, indem wir die Gruppe in unzerlegbare Bausteine (zyklische Gruppen) zerlegt haben.

Verallgemeinerung (ohne Beweis):

SATZ A:

Für eine Primzahl p ungleich 2, eine natürliche Zahl a größer gleich 2 und eine ganze Zahl g sind folgende drei Aussagen äquivalent:

1) g ist Primitivwurzel modulo p^a.

2) g ist Primitivwurzel modulo p und $g^{(p-1)}$ ist nicht kongruent zu 1 modulo p^2.

3) g ist Primitivwurzel modulo p^2.

SATZ B:

Ist p eine Primzahl ungleich 2, g eine ganzzahlige Primitivwurzel modulo p (deren Existenz haben wir bereits bewiesen),

a) so ist g eine Primitivwurzel modulo p^a, für alle a größer gleich zwei, falls $g^{(p-1)}$ nicht kongruent ist zu 1 modulo p^2.

b) so ist $g + p$ eine Primitivwurzel modulo p^a, für alle a größer gleich zwei, falls $g^{(p-1)}$ kongruent ist zu 1 modulo p^2.

Zu 2):

§ 3 Prüfcodes

Als erstes Beispiel haben wir die Europäische Artikelnummer (EAN) betrachtet. Die EAN ist 13-stellig.

Beispiele für typische EANs:

40 28700 071010 Immenhof Honig

40 08535 264948 Reisetti Kochbeutel-Reis (Plus)

40 00345 060888 neuform Gemüsebrühe usw.

Was bedeuten die Ziffern?

Die ersten beiden Ziffern bilden die Länderkennzahl, die folgende vierstellige Nummer ist die Betriebsnummer, die darauf folgende fünfstellige Nummer ist die Artikelnummer und bei der letzten Zahl handelt es sich um die so genannte Prüfziffer.

EAN- Länderkennzahlen:

00-09	USA, Kanada	73	Schweden
30-37	Frankreich	76	Schweiz
40-43	Deutschland	80-81	Italien
49	Japan	84	Spanien
50	Großbritannien	87	Niederlande
54	Belgien	90-91	Österreich
57	Dänemark	93	Australien
64	Finnland	60	Südafrika
70	Norwegen	978	Bücher

Wie funktioniert das Prüfverfahren?

Vorgehen: Man multipliziert die Ziffern der EAN (bis auf die letzte) abwechselnd mit eins und drei, die so neu entstandenen Ziffern summiert man auf. Die erhaltene Summe muss nun bei der Division durch zehn null ergeben.

Erkennt die Prüfziffer alle Fehler?

Fehler	Fehlerentdeckrate
Ziffer vergessen	100,00%
Ziffer zuviel eingetippt	100,00%
Ziffer mit Nachbarn vertauscht	88,88%
Ziffernblöcke vertauscht	0,00%
Ziffer falsch eingetippt	100,00%
2 Ziffern falsch eingetippt	90,00%

Beträgt die Fehlerentdeckrate eines Fehlers 100%, so deckt das Prüfverfahren den Fehler in jedem Fall auf.

Welche Fehler tauchen häufig auf? Und wie häufig? Hier das Ergebnis einer statistischen Untersuchung:

Fehlertyp	*Häufigkeit*
Zu viele oder zu wenige Ziffern	25%

Vertauschen benachbarter Ziffern	5%
Vertauschen benachbarter Zweierblöcke	1%
Eine Ziffer falsch	60%
Zwei oder mehr Ziffern falsch	8%

Problem dieser Tabelle: Man weiß nicht unter welchen Bedingungen die Fehler passieren, ob beim Eintippen der EAN in die Kasse oder beim Einlesen durch einen Scanner o.ä..

Elementare Zahlentheorie WS 2003/04

Stundenprotokoll zum 21.11.2003 (MP)

[Zurück zur Protokollübersicht]
[Dieses Protokoll ist noch nicht redigiert.]

Mögliche Fehler:

(a) eine Ziffer vergessen oder zuviel
(b) eine Ziffer falsch
(c) Ziffer mit Nachbarn vertauscht
(d) Ziffernblöcke vertauscht
(e) Mehr als eine Ziffer falsch

(c) ...dd'...

Annahme: Der Fehler wird nicht entdeckt.

= 0
= 0
= 0 ( ) = q * 10 | : 2
= 0

Für folgende d, d' werden die Fehler nicht entdeckt:

d	d'	d – d' = 0
0	5	
1	6	
2	7	
3	8	
4	9	

Fazit: 10 Fehler von 100 werden nicht erkannt.

(d) Dieser Fehler wird nicht entdeckt.

(e) 1. Fall: und sind falsch.

(* 1 + * 3 + * 1 + * 3 + ... + p) = 0

(+ + + 3 * + p) = 0

(+ + + -) = 0

□(□+□-□-□)□= 0.

Wenn der Fehler nicht entdeckt wird, gilt die letzte Zeile.

2. Fall: □ und □ sind falsch.

3. Fall: □ und □ sind falsch.

Die Rechnung für den 2. und 3. Fall verläuft analog.

Fehlerentdeckrate (FER) [Wie viele Fehler werden prozentual entdeckt?]

FER := Anzahl der entdeckten Fehler □ * 100 % [□= □ - □].

Anzahl der möglichen Fehler □

(a) FER: □ = □, also ist die FER = 100 %.

(b) FER = 100 %.

(c) FER = 89 %.

(d) FER = 0 %.

(e) EAN – Code: □... □p

□

□

Fragen: Wie viele Fehler kann man machen, damit der Fehler nicht entdeckt wird?

Welche Möglichkeiten gibt es?

Wir suchen nun zu einem fest gegebenen □ und □ einen zweiten Fehler, so dass der Fehler nicht entdeckt wird.

Möglichkeiten: □ = 12 * 1 = 12

□ = 12 * 9 = 108

FER = □ * 100 % = □ * 100 % = □ * 100 % = 89 %

Welche Fehler tauchen häufig auf? Und wie häufig? Hier ist das Ergebnis einer statistischen Untersuchung:

Fehlertyp	Häufigkeit
(a) Zu viele oder zu wenige Ziffern	25 %
(b) Eine Ziffer falsch	60 %

(c) Zwei oder mehr Ziffern falsch	8 %
(d) Vertauschen benachbarter Zweierblöcke	1 %
(e) Zwei oder mehr Ziffern falsch	8 %

Der Balkencode für die EAN

Der EAN – Code tritt immer zusammen mit dem Balkencode auf.

Frage: Wofür stehen die Balken?

Antwort: Die Balken stellen die unten stehende Zahl dar.
Die Balken stehen für die 1 (schwarzer Balken) und die 0 (weiße Balken).

Der Balkencode wird vom Scanner gelesen. Gleichzeitig wird so der Wareneingang und -ausgang kontrolliert.

In der Schule bietet der Balkencode einen guten Einstieg in die Einführung des Binärsystems.

Auffälligkeiten des Codes:

- Doppelstriche: Rand- und Trennstriche zwischen den Blöcken 101 – 01010 – 101.
- Die erste Ziffer der Länderzahl steht außerhalb des Balkencodes.
- Es gibt verschiedene Darstellungen für dieselben Ziffern, also gibt es verschiedene Codes.
  Im ersten Block wird zwischen den beiden Codes A und B gewechselt, während in der zweiten Hälfte allein der Code C benutzt wird.

Jede Ziffer besteht aus zwei „Doppelstreifen“, je zwei dunkle Streifen sind durch zwei weiße Zwischenräume getrennt.

Codierung der Ziffern

Ziffer	**Code A**	**Code B**	**Code C**
0	0001101	0100111	1110010
1	0011001	0110011	1100110
2	0010011	0011011	1101100
3	0111101	0100001	1000010
4	0100011	0011101	1011100
5	0110001	0111001	1001110

6	0101111	0000101	1010000
7	0111011	0010001	1000100
8	0110111	0001001	1001000
9	0001011	0010111	1110100

Bemerkung. Code A ist das Negative von Code C, Code B und Code C sind spiegelverkehrt.
Der Vorteil besteht darin, dass man keine komplett neue Darstellung für jeden Code haben muss.
Code A und Code B beginnen mit einem hellen Streifen (0) und enden mit einem dunklen Streifen (1), bei Code C ist es genau umgekehrt.
Die Codes sind bewusst so gewählt, dass der Computer auch erkennen kann, ob die Streifen mit dem Lesegerät von rechts nach links oder umgekehrt gelesen werden – unterschiedliche Leserichtungen können also nicht zu Verwechslungen führen!

Im ersten Block der EAN wird die erste EAN-Ziffer „versteckt“. Die umständliche Codierung der ersten EAN-Ziffer war erforderlich, damit EAN-Strichcode-Leser auch die in den USA verwendeten UPC-Strichcodes verarbeiten können: Die erste Ziffer ist nämlich dem UPC-System hinzugefügt worden.

1. Ziffer	**Code-Muster für die linke Seite**
0	AAAAAA
1	AABABB
2	AABBAB
3	AABBBA
4	ABAABB
5	ABBAAB
6	ABBBAA
7	ABABAB
8	ABABBA
9	ABBABA

Strategie zur Entschlüsselung eines Codes

1. Rand- und Trennstriche einzeichnen.

2. Trennstriche zwischen den Ziffern markieren.
3. Anfang und Ende bestimmen.

Zur vorangehenden Stunde (20.11.03),
zur nächsten Stunde (25.11.03),
zur Protokollübersicht.

Elementare Zahlentheorie

Stundenprotokoll vom 25.11.2003 (AW)

[Zurück zur Protokollübersicht]
[Zum Teil 1) der Stunde Hausaufgabe 5]
[Zum Teil 2) der Stunde Hausaufgabe 4]
[Zum Teil 3) der Stunde § 4]

1) Besprechung von Hausaufgabe 5: „Neue Kernlehrpläne“

In den Kernlehrplänen wird das eigenständige Lernen mehr betont als der bloße fachliche Inhalt.

Dieser befindet sich jedoch in den sogenannten Richtlinien und Lehrplänen der einzelnen Fächer.

(Download: http://www.ritterbach.de).

Als Kritik an den Kernlehrplänen wird jedoch genannt, dass diese sowohl für Lehrer als auch für Schüler

zu schwer umsetzbar sind.

In der Schule reicht nach unseren Erfahrungen bislang die bloße Anwendung aus, Schüler lernen viel auswendig

und müssen die Herleitung meist nicht kennen. Schüler sollen jedoch Zusammenhänge erkennen lernen.

Man müsste den Unterricht (und die Klausuren) bereits ab der 5. Klasse grundlegend ändern.

Dieser Umbruch ist jedoch das Schwierigste an der Umsetzung der neuen Kernlehrpläne, schließlich müssen sowohl

berufserfahrene Lehrer von diesen neuen Methoden überzeugt werden, aber auch Eltern der Schüler

und Schülerinnen müssen die Notwendigkeit der neuen Methoden verstehen.

Außerdem diskutierten wir den Punkt, dass bereits in der Ausbildung der Lehrer an der Hochschule

Änderungen stattfinden müssen. Die Fachdidaktik sollte neben den fachspezifischen Veranstaltungen

mehr in den Vordergrund treten als bisher. Dies wird auch mit der neuen Lehrerprüfungsordnung versucht.

2) Besprechung von Hausaufgabe 4:

Zu Aufgabe 4 c):

Vor:
Z/**nZ** als addidtive Gruppe

Beh:
1. Es gibt eine Untergruppe U von **Z** mit der Eigenschaft, dass W= **U**/**nZ** und **nZ** ist Untergruppe von U.
2. Es gibt ein m aus $\mathbf{N_0}$ mit U= **mZ**.

Beweis:

1) W = $\{t_1, t_2, ...\}$ mit t_i aus **Z**/**nZ**.

W als Untergruppe besteht also aus gewissen "Töpfen", das gesuchte U aus Elemeten von **Z** .
Setze U als die Vereinigung aller Töpfe, die in W sind. Zeige dann, dass gilt:

1. **nZ** ist eine Untergruppe von U.
   Beweis: Da t_0 := 0 + **nZ** in W liegt, kann man **U**/**nZ** = {u + **nZ**; u ist Element von U} bilden.
2. U ist Untergruppe.
3. W = **U**/**nZ** (hier sind die beiden Inklusionen zu zeigen):
   a) W ist Untergruppe (oder gleich) **U**/**nZ**.
   b) **U**/**nZ** ist Untergruppe (oder gleich) W.
   Beweis zu a: Es sei t ein Element aus W, somit liegt t in U. t hat die Form: t= x+**nZ** für ein x aus **Z**.
   Also ist auch x aus U und somit ist x+**nZ** Element von **U**/**nZ**.
   Beweis zu b: Geht entprechend.

2) Dies ist die Aussage von Aufgabenteil b).

3) Neuer Paragraf

§4 Quadrate in Z/nZ

Ein Element a* von **Z**/**nZ** heißt Quadrat, wenn ein b* von **Z**/**nZ** existiert mit $b^{*2} = a^*$.

Frage: „Wann“ ist a* aus **Z**/**nZ** ein Quadrat?

Planen:

Vorschläge:
1. Wurzeln berechnen in **Z, Q, R, C** (Und dann?)
2. Umgekehrt: Man nimmt alle *b* und rechnet dann die Quadrate modulo *n* aus.

Tabelle:

n \ b	1	2	3	4	5	6	7	8	9	10	11	12	13
1	0	1											
2	0	1											
3	0	1	1										
4	0	1	0	1									
5	0	1	4	4	1								
6	0	1	4	3	4	1							
7	0	1	4	2	2	4	1						
8	0	1	4	1	0	1	6	1					
9	0	1	4	0	7	7	0	4	1				
10	0	1	4	9	6	5	6	9	4	1			
11	0	1	4	9	5	3	3	5	9	4	1		
12	0	1	4	9	4	1	0	1	4	9	4	1	
13	0	1	4	9	3	12	10	10	12	3	9	4	1
17	0	1	4	9	16	8	2	15	13				

Zum Seitenanfang,
zur vorangehenden Stunde (21.11.03),
zur Protokollübersicht,
zur nächsten Stunde (27.11.03).

Elementare Zahlentheorie:
Stundenprotokoll vom 27.11.2003 (TF)

[Zurück zur Protokollübersicht]
[Dieses Protokoll ist noch nicht redigiert.]

INHALT:

Punkt 1 der Veranstaltung war der letzte Teil des Referates zum Thema: "Prüfcodes" (§ 3), hier: ISB-Nummern.

Zunächst wurde über die vergangene Veranstaltung resümiert und festgestellt, dass beim EAN-Code zahlreiche Fehler auftreten, die nicht erkannt werden.

Es stellte sich also die **Frage** nach Verbesserungsmöglichkeiten hinsichtlich der Fehlererkennung. Folgende beiden **Ideen** wurden genannt: Statt der alternierenden Multiplikation nur mit den Ziffern *1* und *3* sollen mehrere verschiedene Zahlen verwendet werden, und die Rechnung *modulo 10* aus dem EAN-System soll ersetzt werden durch eine Rechnung *modulo p*, wobei *p* eine Primzahl ist. Davon erwarteten wir eine mögliche Verbesserung der Fehleraufdeckungsrate.

Nun wurde eine ISB-Nummer als Beispiel vorgestellt:

3-426-04175-8.

Die erste Ziffer gibt das Land bzw. die Sprache an. Die zweite Zahl steht für den Verlag und die dritte für den Titel des Buches. Die letzte Zahl ist (wie bei EAN) eine Prüfziffer. Dies ergibt neun Ziffern plus die Prüfziffer. Die ersten neun Ziffern werden absteigend mit zehn, neun, acht, etc. multpliziert, also die neunte mit zwei. Diese neun Produkte werden addiert, und die anschließende Addition mit der Prüfziffer muss eine Zahl ergeben, welche *modulo 11* gerechnet werden kann und Null ergibt. In obigem Beispiel ergibt dies die Zahl *187*, welche durch elf teilbar ist.

Nun wurden fünf mögliche Fehlertypen und die Aufdeckungsrate durch die ISBN genannt:

a.) Ziffern werden vergessen bzw. es gibt zu viele Ziffern: *100%*.

b.) Eine Ziffer ist falsch: *100%*.

c.) Ziffern werden mit dem Nachbar vertauscht: *100%*.

d.) Ziffernblöcke werden vertauscht.

e.) Mehr als eine Ziffer wird vertauscht.

Fehler bei den Punkten d. und e. werden in den meisten Fällen aufgedeckt.

Beweis von Punkt c:

Eine ISBN hat die Darstellung $d_9d_8d_7d_6d_5d_4\ d_3d_2d_1p$.

p ist also die negative Summe der Produkte $[d_i\ (i+1)]$ *modulo 11*, wobei i von *1* bis *9* geht.

Es gilt $(i + 1)d_i + i\ d_{i - 1} = z$, wobei z genau eine bestimmte natürliche Zahl ist (denn die letztendliche Summe muss ja durch elf teilbar sein) und i hier größer als zwei ist. Bei Vertauschung der beiden Ziffern müsste also gelten:

$(i + 1)\ d_{i - 1} + i\ d_i = z$. Der Fall $d_i = d_{i - 1}$ ist kein Fehler.

Also gilt: $(i + 1)\ d_i + i\ d_{i-1} - (i + 1)\ d_{i - 1} - i\ d_i = 0$.

$(d_{i + 1} - d_i)\ (i + 2 - i - 1) = 0$.

Also ist $d_{i + 1} = d_i$.

Das bedeutet also, dass alle Fehler (bezüglich Punkt c.) entdeckt werden.

Insgesamt ist dieses System also effizienter bei der Fehleraufdeckung wie EAN. Dieses wird aber weiterhin genutzt, da es zu aufwendig wäre, überall neue Nummerntastaturen zu integrieren, da man bei den ISBN ein *x* benötigt für die Prüfziffer.

Das Thema "Prüfcodes" kann durchaus im Schulunterricht genutzt werden. Mathematisch steht hauptsächlich die "Division mit Rest" dahinter. Der Schüler lernt ein ganz neues Rechensystem kennen. Im Geist können die Schüler völlig neue Objekte entwickeln. Dadurch macht man im jungen Alter einen Niveausprung (von der zweiten auf die dritte "Diskursebene").

Der Lehrer wird es allerdings wegen der enormen Menge von Stoff schwierig haben, weil die Recherchen sehr zeitaufwendig sind.

Punkt 2 der Veranstaltung war § 4, die sogenannten "Quadrate" in Z/nZ. (Es sei Z die Menge der ganzen Zahlen.) Dabei wurde die Tabelle aus der vergangenen Veranstaltung wieder in den Blickpunkt genommen:

n \ b	0	1	2	3	4	5	6	7	8	9	10	11
1	0	1										
2	0	1										
3	0	1	1									
4	0	1	0	1								
5	0	1	4	4	1							
6	0	1	4	3	4	1						
7	0	1	4	2	2	4	1					
8	0	1	4	1	0	1	4	1				
9	0	1	4	0	7	7	0	4	1			
10	0	1	4	9	6	5	6	9	4	1		
11	0	1	4	9	5	3	3	5	9	4	1	
12	0	1	4	9	4	1	0	1	4	9	4	1

Die Einträge sind die Ergebnisse der Rechnung b^2 *modulo n.*

Man erkennt, dass nur gewisse Reste Quadrate sind. Außerdem sieht man eine Spiegelung in den Zeilen (Im Falle von *modulo 5* ist z.B. das Negative von *4* gleich *1*.)

Es stellt sich die **Frage**: "Tritt *a* als Rest eines Quadrates *modulo n* auf, wenn ich *a modulo n* rechne für eine Zahl *a* aus *Z*?" Die Tabelle kann dies nicht klar darstellen.

Plan: Ich formuliere die Frage um: "Ist eine gewisse Funktion surjektiv, so dass *a* als "Bild" getroffen wird?"

Es sei $q := (\bar{x} \to \bar{x}^2)$: *Z/nZ -> Z/nZ.* Es bleibt die Frage: Liegt *a* im Bild von *q*?

Wir studieren *q*:

Frage 1: Ist *q* Homomorphismus (also strukturerhaltend) als Abbildung von Ringen-mit-1?

Prüfung: $(\bar{x} + \bar{y})^2 = \bar{x}^2 + 2\,\overline{xy} + \bar{y}^2$. Dies ist nicht gleich $\bar{x}^2 + \bar{y}^2$. Also ist es kein Homomorphismus zwischen Ringen-mit-1.

Frage 2: Ist *q* ein Monoidhomomorphismus?

Frage 3: Ist *q´*: *E (Z/pZ) -> E (Z/pZ)* ein Gruppenhomomorphismus?

Frage 2 wird mit ja beantwortet, denn: $\overline{xy}$ wird durch *q* auf $\overline{xy}^2$ abgebildet, und dies ist gleich $\bar{x}^2\bar{y}^2$. *(1 ->* $\bar{1}^2 = \bar{1}$*.)*

Frage 3 wird ebenfalls mit ja beantwortet: $\bar{x}^{-1} \to (\bar{x}^{-1})^2 = (\bar{x}^2)^{-1}$.

Nun ergeben sich weitere Fragen, z.B. über Kern und Bild der Abbildungen *q* und *q´*. Diese werden in der nächsten Veranstaltung thematisiert.

Wir machen folgende Definition: Kern $q' := \{\bar{x}$ *aus E (Z/pZ) /* $\bar{x}^2 = 1\}$, und Bild $q' := \{\bar{y}$ *aus E (z/pZ) / Es existiert* $\bar{x}$ *mit* $\bar{x}^2 = \bar{y}\}$.

Kern und Bild von *q´* sind Untergruppen von *E*. *E / Kern q´* ist isomorph zu E^2.

Zur vorangehenden Stunde (25.11.03),
zur nächsten Stunde (28.11.03),
zur Protokollübersicht.

§4 Quadrate in $E(\mathbb{Z}/n\mathbb{Z})$

Wir wollen die Quadratzahlen in $E(\mathbb{Z}/n\mathbb{Z})$ studieren. Dabei betrachten wir insbesondere den Fall $E(\mathbb{Z}/p\mathbb{Z})$ für eine Primzahl p. Wie bereits bekannt, ist

$$E := E(\mathbb{Z}/p\mathbb{Z}) \cong C_{p-1},$$

also

$$E = \langle \bar{t} \rangle$$

für ein $\bar{t} = t + p\mathbb{Z} \in E(\mathbb{Z}/p\mathbb{Z}) \setminus \{p\mathbb{Z}\}$. Die Zahl $t \in \mathbb{Z}$ heißt dann Primitivwurzel modulo p. Die Menge der Quadrate aus E sei im Folgenden mit E^2 bezeichnet. Es ist

$$E^2 = \{\bar{x}^2 \in E \mid \bar{x} \in E\} \leq E.$$

Einen Ansatz liefert der Gruppen-Homomorphismus

$$\sigma := (\bar{x} \mapsto \bar{x}^2) \colon E \to E.$$

Der Kern zu diesem Gruppen-Homomorphismus ist gegeben durch

$$\mathrm{Kern}(\sigma) = \{\bar{x} \in E \mid \bar{x}^2 = \bar{1} = 1 + p\mathbb{Z}\} = \langle -\bar{1} \rangle$$

Nach dem Homomorphiesatz für Gruppen gilt nun

$$E/\langle \bar{1} \rangle > = E/\mathrm{Kern}(\sigma) \cong \mathrm{Bild}(\sigma) = E^2,$$

woraus

$$|E^2| = |E/\langle \bar{1} \rangle| = \frac{p-1}{2}$$

folgt. Doch welche Elemente liegen nun in E^2? Gibt es zu einem gegebenen $\bar{a} \in E$ ein $\bar{b} \in E$ mit $\bar{a} = \bar{b}^2$?

Ist zum Beispiel stets $\bar{a} = -\bar{1} \in E^2$? - Dem ist nicht so, es ist etwa

$$\langle \bar{1} \rangle > \leq E(\mathbb{Z}/5\mathbb{Z})^2,$$

aber

$$\langle \bar{1} \rangle > \not\leq E(\mathbb{Z}/7\mathbb{Z})^2.$$

Definition 1 ***(Legendre-Symbol)***
Es seien $a \in \mathbb{N}$ beliebig, p eine Primzahl und $E^2 := \{\bar{x}^2 \in E(\mathbb{Z}/p\mathbb{Z}) \mid \bar{x} \in E(\mathbb{Z}/p\mathbb{Z})\}$. Wir setzen

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & \text{falls } \bar{a} \in E^2, \\ -1, & \text{falls } \bar{a} \notin E^2. \end{cases}$$

Für $p = 7$ ergibt sich zum Beispiel

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1 \text{ und } \left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1.$$

Satz 1 ***(Eigenschaften von*** $\left(\frac{a}{p}\right)$***)***
Es seien $a, b \in \mathbb{N}$ beliebig sowie p eine Primzahl.
(1) Aus $a \equiv b \bmod p$ folgt $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
(2) Für alle $a \in \mathbb{Z}$ ist $\left(\frac{a^2}{p}\right) = 1$.
(3) Es ist $\left(\frac{1}{p}\right) = 1$.
(4) $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
Beweis. Es sei $E := E(\mathbb{Z}/p\mathbb{Z})$ und $E^2 := \{\bar{x}^2 \in E \mid \bar{x} \in E\}$.
(1) Aus $a \equiv b \bmod p$ folgt $\bar{a} = \bar{b}$ und damit $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) Für alle $a \in \mathbb{Z}$ ist $\overline{a^2} = \bar{a}^2 \in E^2$, also $\left(\frac{a^2}{p}\right) = 1$.

(3) Es ist $\bar{1} = \bar{1}^2 \in E^2$, somit folgt $\left(\frac{1}{p}\right) = 1$.

(4) Da $|E^2| = \frac{p-1}{2}$ ist, folgt $[E : E^2] = 2$, also

$$E = E^2 \dot{\cup} \bar{t}E^2.$$

(Es gibt kein $\bar{x} \in E$ mit $\bar{t} = \bar{x}^2$, denn $o(\bar{t}) = |E|$.)
1. Fall: Es sei $\bar{a}, \bar{b} \in E^2$. Dann ist $\bar{a}\bar{b} = \overline{ab} \in E^2$, also folgt

$$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = 1 \cdot 1 = 1 = \left(\frac{ab}{p}\right).$$

2. Fall: Es sei $\bar{a}, \bar{b} \notin E^2$. Dann ist $\bar{a}\bar{b} = \overline{ab} \in E^2$, also folgt

$$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = (-1) \cdot (-1) = 1 = \left(\frac{ab}{p}\right).$$

3. Fall: Es sei $\bar{a} \in E^2, \bar{b} \notin E^2$. Dann ist $\bar{a}\bar{b} = \overline{ab} \notin E^2$, also folgt

$$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = 1 \cdot (-1) = -1 = \left(\frac{ab}{p}\right). \qquad ||$$

Bemerkung 1 Die Abbildung

$$\left(\frac{\cdot}{p}\right) := (a \mapsto \left(\frac{a}{p}\right)) \colon \mathbb{Z} \setminus \{0\} \to \{\pm 1\}$$

ist also ein Monoidhomomorphismus.

Satz 2 ***(Eulers Kriterium)***
Es sei $p \neq 2$ eine Primzahl und $a \in \mathbb{Z} \setminus p\mathbb{Z}$ beliebig. Dann gilt

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

Beweis. Es sei $\bar{a} \in E := E(\mathbb{Z}/p\mathbb{Z})$ beliebig. Dann ist

$$\bar{a}^{p-1} = \bar{1},$$

denn $o(\bar{a}) \mid p-1$. Daraus folgt

$$(\bar{a}^{\frac{p-1}{2}} - \bar{1}) \cdot (\bar{a}^{\frac{p-1}{2}} + \bar{1}) = \bar{a}^{p-1} - \bar{1} = \bar{0},$$

also, da $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist,

$$\bar{a}^{\frac{p-1}{2}} \in \{\pm 1\}.$$

1. Fall: Es sei $\left(\frac{a}{p}\right) = 1$. Dann gibt es also ein $\bar{x} \in E$ mit $\bar{a} = \bar{x}^2$. Somit folgt

$$\overline{a^{\frac{p-1}{2}}} = \bar{a}^{\frac{p-1}{2}} = (\bar{x}^2)^{\frac{p-1}{2}} = \bar{x}^{p-1} = \bar{1}$$

und damit

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

2. Fall: Es sei $\left(\frac{a}{p}\right) = -1$. Weiter sei $\bar{t} \in E$ mit $E = <\bar{t}>$. Dann ist

$$\bar{a} = \bar{t}^k \text{ für ein ungerades } k \in \{0, \ldots, p-1\}.$$

Außerdem ist $\bar{t}^{\frac{p-1}{2}} = -\bar{1}$ das Element der Ordnung 2 in E. Daraus folgt

$$\overline{a^{\frac{p-1}{2}}} = \bar{a}^{\frac{p-1}{2}} = (\bar{t}^j)^{\frac{p-1}{2}} = (\bar{t}^{\frac{p-1}{2}})^j = (-\bar{1})^j = -\bar{1},$$

also

$$a^{\frac{p-1}{2}} \equiv -1 \bmod p. \qquad ||$$

Beispiel 1 Es sei $a = -1$ und p eine Primzahl. Dann ist

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & \text{für } p \equiv 1 \bmod 4, \\ -1, & \text{für } p \equiv 3 \bmod 4, \end{cases} \quad \bmod p.$$

Satz 3 ***(quadratisches Reziprozitätsgesetz von Legendre und Gauss)***
Es seien $p, q \neq 2$ Primzahlen mit $p \neq q$. Dann ist

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

Beweis. Siehe Literatur über Elementare Zahlentheorie. ||

Beispiel 2 *Es ist*

$$\begin{aligned}
\left(\frac{23}{59}\right) &= \left(\frac{59}{23}\right)\cdot(-1)^{29\cdot 11} \\
&= (-1)\cdot\left(\frac{13}{23}\right) \\
&= (-1)\cdot\left(\frac{23}{13}\right)\cdot(-1)^{11\cdot 6} \\
&= (-1)\cdot\left(\frac{10}{13}\right) \\
&= (-1)\cdot\left(\frac{-3}{13}\right) \\
&= (-1)\cdot\left(\frac{-1}{13}\right)\left(\frac{3}{13}\right) \\
&= (-1)\cdot\left(\frac{13}{3}\right)\cdot(-1)^{6\cdot 1} \\
&= (-1)\cdot\left(\frac{1}{3}\right) \\
&= -1.
\end{aligned}$$

Satz 4 ***(zweite Komplementärformel)*** Es sei $p \neq 2$ eine Primzahl. Dann ist

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Beweis. Siehe Literatur über Elementare Zahlentheorie. ||

§6 Der Hauptsatz der Arithmetik

Frage 1 Warum gilt der Satz über die Existenz und Eindeutigkeit der Darstellung von natürlichen Zahlen als Produkt von Primzahlen?

Frage 2 Was ist eine Primzahl?

Satz 5 $\sqrt{2}$ ist eine irrationale Zahl.
Beweis. (nach Euklid, ca. 340 - 270 v. Chr.)
Angenommen, $\sqrt{2}$ ist eine rationale Zahl. Dann gibt es $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$, so dass

$$\sqrt{2} = \frac{m}{n}.$$

Es folgt

$$2 = \frac{m^2}{n^2}$$

also

$$m^2 = 2n^2.$$

Dann gilt aber $2 \mid m$, es gibt also ein $x \in \mathbb{N}$ mit $m = 2x$. Somit erhalten wir

$$4x^2 = 2n^2$$

also

$$2x^2 = n^2,$$

also $2 \mid n$ im Widerspruch dazu, dass $\mathrm{ggT}(m, n) = 1$ ist. ||

Zur Erinnerung:

Definition 2 ***(größter gemeinsamer Teiler)***
Es seien M ein Monoid und $a, b \in M$. Ein größter gemeinsamer Teiler von a, b ist ein $g \in M$ für das gilt:
(1) $g \mid a$ und $g \mid b$.
(2) Ist $u \in M$ mit $u \mid a$ und $u \mid b$, so folgt $u \mid g$.

Der Beweis zum vorigen Satz benutzte die Existenz und Eindeutigkeit der Primfaktorzerlegung einer natürlichen Zahl.
Gilt in $\mathbb{N}$ stets „aus $2 \mid xy$ folgt $2 \mid x$ oder $2 \mid y$“?

Definition 3 ***(unzerlegbare Elemente)***
Es sei M ein Monoid. Ein Element $u \in M$ heißt *unzerlegbar*, wenn
(1) u kein Nullelement ist ($n \in M$ heißt Nullelement, wenn $nx = n$ für alle $x \in M$),
(2) $u \notin E(M)$ ist und
(3) aus $u = ab$ folgt, dass $a \in E(M)$ oder $b \in E(M)$ ist.

Definition 4 ***(prime Elemente)***
Es sei M ein Monoid. Ein Element $p \in M$ heißt *prim*, wenn
(1) p kein Nullelement ist,
(2) $p \notin E(M)$ ist und
(3) aus $p = ab$ folgt, dass $p \mid a$ oder $p \mid b$.

Frage 3 Ist unzerlegbar gleich prim in allgemeinen Monoiden?

Beispiel 3 (1) In $\mathbb{N}$ ist unzerlegbar gleich prim. Ebenso in $M_1 := 2\mathbb{N}_0 + 1$ und
$M_2 := 3\mathbb{N}_0 + 1$.
(2) Betrachten wir jedoch als Gegenbeispiel

$$M := 2\mathbb{N}_0 \cup \{1\}.$$

In diesem Monoid ist 42 unzerlegbar (denn $21 \notin M$), aber nicht prim, denn

$$420 = 6 \cdot 70$$

und

$$42 \nmid 6 \text{ und } 42 \nmid 70.$$

Frage 4 Woran liegt es, dass in $\mathbb{N}$ unzerlegbare Element auch prim sind (und umgekehrt), in allgemeinen Monoiden jedoch nicht?

[Zurück zur Protokollübersicht]
[Dieses Protokoll ist noch nicht redigiert.]

Stundenprotokoll zur Vorlesung Elementare Zahlentheorie vom 04.12.2003 (DB)

Fortsetzung von §6. Der Hauptsatz der Arithmetik

Wir waren von der Definition von unzerlegbaren Elementen und primen Elementen zu einigen Fragen gekommen.

Fage: Sind unzerlegbare Elemente gleich primen Elementen in einem kommutativen Monoid?

Definition: Kürzungsregel nennt man die Eigenschaft, dass aus $a \cdot x = a \cdot y,\ a \neq 0$ folgt $x = y$.

$|N$ erfüllt die Kürzungsregel (KR).
$/Z$ erfüllt die KR. $a \cdot (x - y) = 0$, da $/Z$ ohne Nullteiler ist und $a \neq 0$ folgt, dass $x = y$.

Satz 1: M sei ein kommutativer Monoid mit Kürzungsregel. Dann sind alle Primelemente unzerlegbar.

Beweis: Es sei p ein Element in M und p sei prim. [Z.z.: p unzerlegbar]
Nun sei $p = a \cdot b$ in M. [Z.z.: a oder b sind in $E(M)$].
$p|p$, d.h. $p|a \cdot b$, somit folgt $p|a$ oder $p|b$, etwa $p|a$.
Daraus folgt $p \cdot x = a$ für ein $x \in M$.
Daraus folgt $a = p \cdot x = a \cdot b \cdot x$.
D.h. $a = a \cdot b \cdot x$,
daraus folgt $1 = b \cdot x$, somit gilt $b \in E(M)$.

Beispiel: In allen Integritätsbereichen (komm. Ring-m-1 ohne Nullteiler) sind prime Elemente unzerlegbar. Z.B. $K[x]$ für K ein Körper.

Frage: Wann sind unzerlegbare Elemente prim?

In $/Z$: Es sei u unzerlegbar [Z.z.: u prim]
Es sei $u|a \cdot b$. [Z.z. $u|a$ oder $u|b$]
Wenn $u|a$ ist, dann ist man fertig.
Es sei also, dass u a nicht teilt. [Z.z. $u|b$]

Idee: Es sei g der $ggT(u, a)$. [In $/Z$ existiert Division mit Rest, d.h. der EA bricht ab].

D.h.:

1. $g|u$ und $g|a$, wenn
2. $h|u$ und $h|a$, dann folgt $h|g$.
3. $g = \alpha \cdot u + \beta \cdot a$ für geeignete $\alpha, \beta \in /Z$.
   $g \cdot b = \alpha \cdot u \cdot b + \beta \cdot a \cdot b$.

Somit folgt aus $u \mid (u \cdot b)$ und $u \mid (a \cdot b) = u$
$u \mid (g \cdot b)$.
Sei also $u = g \cdot y$, daraus folgt, da u unzerlegbar, dass $g \in /Z$ oder $y \in /Z$
Nun sei o.B.d.A. $g \in /Z$
$u \cdot z = g \cdot b$, daraus folgt $u \cdot z \cdot g^{-1} = b$, daraus folgt $u|b$.
Aber $g|a$, somit $(g \cdot y)|a$ falls $y \in E(/Z)$.
$u|a$, dies ist aber ein Widerspruch zu der Voraussetzung, dass u a nicht teilt.
Somit ist $g \in /Z$

Satz 2: Es sei R ein euklidischer Bereich, d.h. ein Integritätsbereich zusammen mit einer s
genannten "Gradfunktion"
$\delta : R \setminus \{0\} \rightarrow (/N_0, <)$, mit:

Zu jedem Paar (a, b), $a \neq 0$, $b \neq 0$, existiert (q, r) in R mit $a = q \cdot b + r$, wobei $r =$
oder $\delta(r) < \delta(b)$.
Dann sind die unzerlegbaren Elemente in R prim. [prim = unzerlegbar].

Beispiel: $(/Z, | \cdot |)$, $(K[x], Grad)$
[In euklidischen Bereichen bricht der *EA* ab und es gibt den *XEA*.]

Der Hauptsatz der Arithmetik

Satz: In einem euklidischen Bereich (R, δ) gilt:

1. **Existenz:** Jedes Element ungleich Null oder Eins ist das Produkt von unzerlegbaren [=primen] Elementen.
2. **Eindeutigkeit:** Hat ein Element $x \neq 0$, $x \neq 1$ die Darstellung:
   $x = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$ mit unzerlegbaren [=prim] Elementen p_i, q_j, so ist $r = s$ und die p_i stimmen bis auf Reihenfolge und Einheiten mit den q_j überein.

Beweis: Es sei $x \neq 0$, $x \neq 1$ in R.

Existenz Wenn x unzerlegbar, dann sind wir fertig.
Also sei x zerlegbar: $x = a \cdot b$, $a,b \in E(R)$.
Falls a oder b zerlegbar sind, dann zerlege man weiter.
Weil aus $x = a \cdot b$ folgt $\delta(a) < \delta(x)$ endet das Verfahren. [Vgl. späteren Satz]

Eindeutigkeit Es sei $x = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$ mit primen [= unzerlegbaren] Elementen p_i, q_j.
$p_1|x = q_1 \cdot \ldots \cdot q_s$ daraus folgt $p_1|q_i$ und o.B.d.A. kann $p_1|q_1$ angenommen werden, daraus folgt $p_1 \cdot x_1 = q_1$. Da q_1 unzerlegbar ist folgt $x_1 \in E(R)$.
Es folgt mit der KR.:
$y = p_2 \cdot \ldots \cdot p_r = x_1 \cdot q_2 \cdot \ldots \cdot q_s$.
Mit vollständiger Induktion nach minimaler Faktorzahl folgt die Eindeutigkeit bis auf Reihenfolge oder Einheiten aus R.

"Teilen" in der Sprache der Moduln (Kummer 19. Jahrhundert)
Es sei R ein Integritätsbereich, dann heißt
$a|b$ dasselbe wie $a \cdot x = b$ für $x \in R$,
$aR \geq bR$.
Somit ist $a|b$ äquivalent zu $aR \geq bR$ mit$bR = {}_R<b>$

Satz 3: Es sei (R, δ) ein euklidischer Integritätsbereich (z.B. $/Z$, $K[x]$), betrachte R als R-

Modul (R zyklisch, d.h. $R = R\ 1 = <1>_R$). Dann ist auch jedes Teilmodul I von R zyklisch und es existiert $I = mR$ für ein $m \in R$.

Beweis: Wenn $I = \{0\} \leq R$, so ist $I = R \cdot 0$.
Nun sei $I \neq \{0\}$.
Es sei m ein Element minimalen Grades $\delta(m)$ aus I.
Es sei $u \in I$.
Nun mache man eine Divison mit Rest:
u = $q \cdot m + r$, $r = 0$ oder $\delta(r) < \delta(m)$.
Da $u \in I$ und $q \cdot m \in I$ folgt, dass $r \in I$, also ist wegen der Minimalität von m $r = 0$.
Somit ist $u \in mR$; Also $I \subseteq mR$.
$I \supseteq mR$, da $m \in I$.
Daraus folgt $I = mR$.

Zur vorangehenden Stunde (02.12.03),
zur nächsten Stunde (05.12.03),
zur Protokollübersicht.

Vorlesung Elementare Zahlentheorie WS 2003/04
Freitag, den 5.12.03 (AK)

[Zurück zur Protokollübersicht]
[Dieses Protokoll ist noch nicht redigiert.]

kommutativer Ring-m-1: Monoid.

Hauptsatz der Arithmetik: Existenz von Zerlegung als Produkt von unzerlegbaren Elementen.

Eindeutigkeit von Zerlegung als Produkt von primen Elementen

R euklidischer Bereich (R, δ)

R kommutativer Integritätsbereich

$\delta: R \setminus \{0\} \to \mathbb{N}_0$

Idee: a|b in R $\Leftrightarrow Ra \supseteq Rb$

a|echt b $\Leftrightarrow Ra \supset Rb$

Satz4:

Beh: Existenz von Zerlegung als Produkt von unzerlegbaren Elementen gilt in Euklidischen Bereichen.

Bew: (R, δ) euklidischer Bereich. $a \in R \setminus \{0\}$ und $a \notin E(R)$.

Ok, falls keine endliche Kette echter Teiler von a existiert.

$\ldots | a_2 | a_1 | a$ $a \notin R$ existiert.

Wenn eine solche Kette doch existiert, haben wir eine unendliche Kette

$R > \ldots W \geq \ldots > Ra_2 > Ra_1 > Ra$ von zyklischen Teilmodulen.

Bilde $W := \bigcup_{i=1}^{\infty} Ra_i$

ist R-Teilmodul von R. $\overset{\text{Satz3}}{\to} W = Rw$ für ein $w \in W$

Etwa $w \in Ra_k \subset Ra_{k+1} \subset \ldots \subset W = Rw$

$W = Rw \subseteq Ra_k$, $Rw \subset Rw$

(Widerspruch)

Fazit: Hauptsatz der Arithmetik gilt für Euklidische Bereiche.

Allgemeine Definitionen:

R Ring-m-1

$_RR$, R_R , $_RR_R$

Teilmodul: „Linksideal“ , „Rechtsideal“ , „Ideal“ von R.

Zyklische Teilmodule: „Hauptideale“

Euklidische Bereiche sind Hauptidealbereiche.

§7 Analyse des EA, XEA

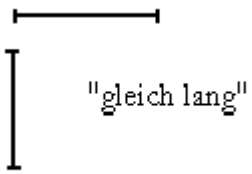
I.Größen

Frage: Was ist ein „Größenbereich“?

z.B. der Größenbereich der Längen?

Physikalische existent: Stellen im Raum

1.Diskursebene



2.Diskursebene: „Kongruent“ ohne math. Definition sondern mithilfe geometrischer Vorstellung.

Was ist den Objekten gemeinsam?

Länge (abstrakt) rein theoretischer Begriff, kein physikalisches Objekt.

Längenbereich: Man kann addieren: komm.Gruppe

Vergleich: < Totalordnung

angeordnete Gruppe:

Zu $0<a<b$ existiert $n \in \mathbb{N}$ mit $na>b$ (Archimedisches Axiom).

(R,>) ist archimedisch angeordnet.

C_R konstante Funktion

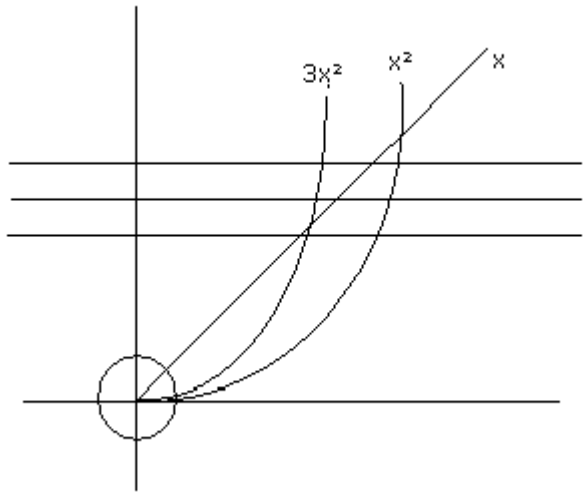
(R[X],<)

f(0)=g(0)=0

$X^3<X^2<X$ auf einem kleinen Intervall

$X^3<3X^2<X$

$a:=x^2 \rightarrow nX^2<X=:b$



Definition: Ein Größenbereich ist eine archimedisch angeordnete (additiv geschreibene) abelsche Gruppe.

Angeordnete Gruppe: (G,+,0,-) Gruppe.

Anordnung (G,<) <: 1) Für $a,b \in G$ gilt genau eine der folgende Aussagen: a<b, a=b, a>b.

2)Aus a<b, b<c folgt a<c.

Angeordnete Gruppe: Zusätzlich: Aus a<b folgt a+c<b+c.

Archimedisch angeordnete Gruppe: ... zu 0<a,b existiert $n \in \mathbb{N}$ mit b<na.

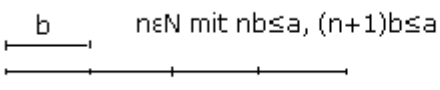
Hilfssatz: In einer angeordneten Gruppe haben alle Elemente ≠0 unendliche Ordnung.

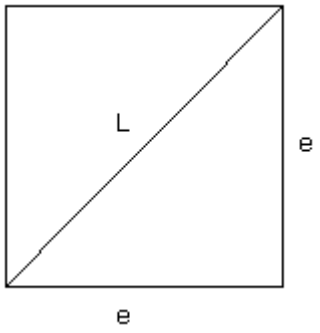
Beweis: Angenommen, a≠0 hat doch endliche Ordnung n: na=0

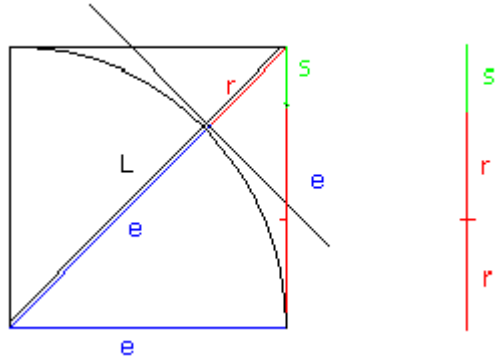
1.Fall: a>0: 0<a<2a<3a<... $\rightarrow$ na≠0.

2.Fall: a<0: analog.

Hilfssatz: In einer archimedisch angeordneten Gruppe haben wir „Division mit Rest“: zu 0<a,b existiert







$Q_e \leq G$ $Z_e \leq G$ „Wechselwegnahme“

d=1e+r
e=2r+s
r=2s+t
s=2t+u
...

nicht endender EA!

Zur vorangehenden Stunde (04.12.03),
zur nächsten Stunde (09.12.03),
zur Protokollübersicht.

[Zurück zur Protokollübersicht]

Das Pentagramm

Vorlesung "Elementare Zahlentheorie" vom 09.12.2003 (NB)

Johann Wolfgang Goethe: "Faust", Der Tragödie erster Teil, Z. 1384 - Z.1408

(...)

MEPHISTOPHELES.
Wir wollen wirklich uns besinnen,
Die nächsten Male mehr davon!
Dürft ich wohl diesmal mich entfernen?

FAUST.
Ich sehe nicht, warum du fragst.
Ich habe jetzt dich kennen lernen
Besuche nun mich, wie du magst.
Hier ist das Fenster, hier die Türe,
Ein Rauchfang ist dir auch gewiß.

MEPHISTOPHELES.
Gesteh ichs nur! daß ich hinausspaziere,
Verbietet mir ein kleines Hindernis,
Der **Drudenfuß** auf Eurer Schwelle

FAUST.
Das **Pentagramma** macht dir Pein?
Ei sage mir, du Sohn der Hölle,
Wenn das dich bannt, wie kamst du denn herein?
Wie ward ein solcher Geist betrogen?

MEPHISTOPHELES.
Beschaut es recht! es ist nicht gut gezogen:
Der eine Winkel, der nach außen zu,
Ist, wie du siehst, ein wenig offen.

FAUST.
Das hat der Zufall gut getroffen!
Und mein Gefangner wärst denn du?
Das ist von ungefähr gelungen!

MEPHISTOPHELES.
Der Pudel merkte nichts, als er hereingesprungen,
Die Sache sieht jetzt anders aus:
Der Teufel kann nicht aus dem Haus.

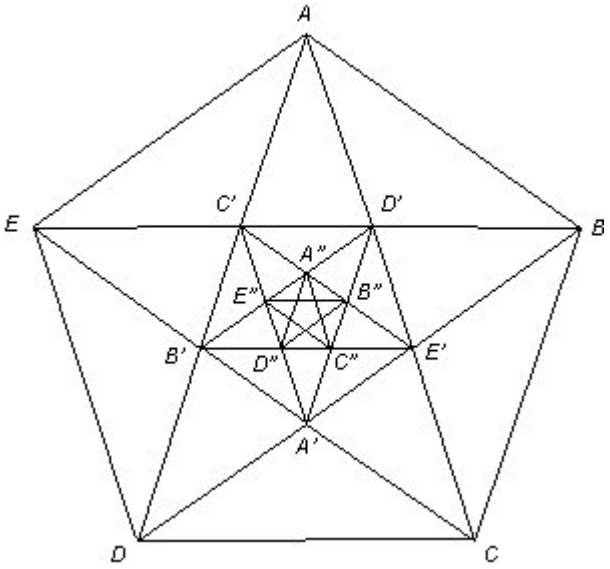
(...)

Doch schon lange vor Goethe war das Pentagramm ein besonderes Symbol:

Die *Phythagoreer* benutzten es ca. 500 v. Chr. als Geheimzeichen für ihren Bund. Die Pythagoreer glaubten, dass zwei gleichartige Größen immer durch ein gemeinsames Maß gemessen bzw. verglichen werden könnten. Ein solches Maß könnte nach ihrer Auffassung immer so gewählt werden, dass beide Größen als ganzzahlige Vielfache dieses Maßes darstellbar sind. Existiert zu zwei Größen ein solches Maß, dann heißen die Größen kommensurabel. Das größte gemeinsame Maß zweier Größen wird durch den *EUKLIDischen Algorithmus* bestimmt. Die dem EUKLIDischen Algorithmus zugrunde liegende Idee der Methode der Wechselwegnahme war vielen Handwerkern zu dieser Zeit schon lange bekannt. Da die Wechselwegnahme im Alltag immer zu einer Lösung führte, vermuteten die Phythagoreer, dass zwei beliebig gewählte, gleichartige Größen immer kommensurabel seien. Nachdem die Pythagoreer um ca. 500. v.Chr. die Mathematik als Wissenschaft begründet hatten, erfuhr sie kurz darauf bereits ihre erste Grundlagenkrise. Diese Krise wurde durch *HIPPASOS VON METAPONT* (ca. 5.Jhd. v. Chr.), einem Mann aus den eigenen Reihen, heraufbeschworen. Der Legende nach soll er am Pentagramm, dem Ordenssymbold der Pythagoreer, entdeckt haben, dass dessen Diagonale und Seitenlänge nicht kommensurabel sind. Da diese Entdeckung die Grundüberzeugung der Pythagoreer, dass sich „alles“ durch (natürliche) Zahlen repräsentieren läßt, in Frage stellte, sollen HIPPASOS Sektenbrüder ihn deshalb ins Meer geworfen bzw. die Götter sollen sogar sein Schiff zerschmettert haben. Die Endeckung inkommensurabler Größen ließ außerdem geometrische Beweise, die die Kommensurabilität für beliebige Größen voraussetzten, nichtig werden.

HIPPASOS´ Beweis soll hier nun dargelegt werden:

[Konvention: Mit *AB* bezeichne ich die Gerade, die durch die Punkte *A* und *B* geht.]



Betrachten wir die **Seite** *e := ED* und die **Diagonale** *d := AC*. *e* und *d* sind parallel zueinander, da im regelm. Fünfeck (Folge von 5 Punkten mit gleich langen Seiten und gleich großen Winkeln) jede Diagonale zu ihrer gegenüberliegenden Seite parallel sind. Dies liegt daran, dass das Fünfeck symmetrisch bspw. zur senkrechten Achse durch *A* ist, d.h., dass *EB* und *DC* senkrecht zu dieser Achse und damit parallel sind usw.

Wir versuchen nun Informationen über das Verhältnis von *d* zu *e* zu erfahren:

Da nun *e* und *d* und auch *DB* und *EA* parallel sind bilden die Punkte *E, D, E´, A* ein Parallelogramm *P*. Also ist auch *e = AE´*. Mit *e´ := B´E´ = E´C* (wieder regelm. Fünfeck) gilt also:

$d = e + e'$

Desweiteren ist $e'' := C'D' = D'E'$ (wieder regelm. Fünfeck, da ähnlich). Betrachten wir das Parallelogramm P', welches durch die Punkte E, D', C, D gebildet wird. Man sieht, dass $e = D'C$. Also:

$e = e' + e''$

Verfahren wir nun so weiter, so ergibt sich:

$e' = e'' + e'''$,

$e'' = e''' + e''''$

(...)

Das Verfahren endet nie, da wir immer wieder neue (ähnliche) Fünfecke finden (s. Zeichnung).

Also ist $d : e$ (das Verhältnis einer Diagonalen zu einer Seitenlänge) irrational.

FRAGE: Welche (irrationale) Zahl repräsentiert denn nun $d : e$?

1. Methode (exakte Berechnung):

$d/e = e/e'$(da die Pentagramme ähnlich sind), $e/d = e'/e = (d - e)/e = d/e - 1$, $d/e = e/d + 1$. Mit $x := d/e$ folgt: $x = 1/x + 1$, $x^2 - x - 1 = 0$, $x = (1 + \sqrt{5}) / 2$.

2. Methode (approximative Berechnung):

Approximation für $v = 0$:

$d = e + r = 8u$,
$e = r + s = 5u$,
$r = s + t = 3u$,
$s = t + u = 2u$,
$t = u + v = u$.

In diesem Beispiel: $d : e \approx 8/5 = 1{,}6$ [zum Vergleich: $(1 + \sqrt{5}) / 2 \approx 1{,}6180$].

Wie man sieht, ergeben die Koeffizienten von u gerade die sog. *Fibbonacci-Folge* [man füge noch eine *1* hinzu]. Von dieser weiß man, dass der Abstand zweier Folgenglieder, also auch der Wert $d : e$, gegen $(1 + \sqrt{5}) / 2$ konvergiert.

ERGÄNZUNG: ÜBERTRAGUNG AUF QUADRATE

Dieses Verfahren kann man, wie in der letzten Vorlesung gesehen, auch auf Quadrate übertragen. Dort konnte man folgende Verhältnisse feststellen:

$d = 1e + r$
$e = 2r + s$
$r = 2s + t$
$s = 2t + u$
usw.

Nun Berechnung nach der approximativen Methode:

$r = 0$ $d = e$ ***d : e ≈ 1***	$s = 0$ $d = e + r = 3r$ $e = 2r$ ***d : e ≈ 3/2= 1,5***	$t = 0$ $d = 1e + r = 7s$ $e = 2r + s = 5s$ $r = 2s$ ***d : e ≈ 7/5 = 1,4***	$u = 0$ $d = 1e + r = 17t$ $e = 2r + s = 12t$ $r = 2s + t = 5t$ $s = 2t$ ***d : e ≈ 17/12 ≈ 1,4167***	$v = 0$ $d = 1e + r = 41u$ $e = 2r + s = 29u$ $r = 2s + t = 12u$ $s = 2t + u = 5u$ $t = 2u$ **d : e ≈ 41/29 ≈ 1,4138**

Wie man sieht nähern sich die Werte immer mehr $\sqrt{2}$ an. Also kann man vermuten [und auch beweisen], dass im Quadrat $d : e = \sqrt{2} : 1$ gilt.

Zur vorangehenden Stunde (05.12.03),
zur nächsten Stunde (11.12.03),
zur Protokollübersicht.

Vorlesung Elementare Zahlentheorie WS 2003/04
Donnerstag, den 11.12.03 (AK)

[Zurück zur Protokollübersicht]
[Das Protokoll ist noch nicht redigiert.]

§8 Analyse des EA/XEA

Teil I: Größen

Teil II: Algebraische Analyse

Schema des EA und XEA:

$$r_i = x_i a + y_i b$$

$a:=r_{-1}$	$1=:x_{-1}$	$0=:y_{-1}$
$b:=r_0$	$0=:x_0$	$1=:y_0$
$r_{-1}-Q_0r_0=:r_1$	$x_{-1}-Q_0x_0=:x_1$	$y_{-1}-Q_0y_0=:y_1$
$r_0-Q_1r_1=:r_2$	$x_0-Q_1x_1=:x_2$	$y_0-Q_1y_1=:y_2$
...	...	...
$r_{n-2}-Q_{n-1}r_{n-1}=:r_n$	$x_{n-2}-Q_{n-1}x_{n-1}=:x_n$	$y_{n-2}-Q_{n-1}y_{n-1}=:y_n$
$r_{n-1}-Q_nr_n=:r_{n+1}$	$x_{n-1}-Q_nx_n=:x_{n+1}$	$y_{n-1}-Q_ny_n=:y_{n+1}$
$r_n-Q_{n+1}r_{n+1}=:r_{n+2}$	$x_n-Q_{n+1}x_{n+1}=:x_{n+2}$	$y_n-Q_{n+1}y_{n+1}=:y_{n+2}$

Fragen

F1: Gilt $r_i=x_ia+y_ib$ für "alle" i?

F2: Was heißt hier "alle"?

F3: Konvergiert die Folge $(r_{-1},r_1,r_2,...)$? Gegen Null?

F4: Spielt die Reihenfolge von a,b eine Rolle bei diesen Fragen, d.h. vgl. Schema zu (a,b) mit Schema zu (b,a).

F5: Was sind die r_i,Q_i,x_i,y_i für Elemente? Was wird vorgeschreiben und was wird dann definiert?

F6: Was bedeutet es (was folgt), wenn $r_{n+1}=0$ ist (eventl. "erstmals")

A6: Sind $a,b,Q_i,r_i \in N_0$ für i=-1,...,n im Schema für EA und ist $r_{n+1}=0$, so ist $g:=r_n$ ein ggT in N_0 von a und b.

Beweis

i)Von unten: Letzte Zeile:$r_n | r_n$ und $0(=r_{n+1})$. Daraus folgt, dass auch $r_n|r_{n-1}$.

Vorletzte Zeile: $r_n | r_{n-1}$ und r_n, d.h. auch $r_n|r_{n-2}$

...

$r_n \mid a=r_{-1}$ und $b=r_0$.

ii)Es sei h|a und h|b in N_0. Z.z. $h|r_n$.
Von oben: Erste Zeile: $h|r_{-1}$ und r_o d.h. auch $h|r_1$

Zweite Zeile: $h|r_1$ und r_0, d.h. $h|r_2$
...
$h|r_n$

Erinnerung:

Definition: g ist ein ggT in M von (a,b) wenn g|a und g|b gilt und für ein weiteres k mit k|a und k|b gilt: k|g.

F:Wo bin ich?
A:In einem Kommutativen Monoid M (.,1) mit Kürzungsregel.

F:Wie eindeutig ist ein ggT?
A:Es seinen g,k ggT's von (a,b) in M.
Es folgt g|k und k|g,d.h. k=gx und g=ky für gewisse (es existieren) $x,y \in M$.
Einsetzten ergibt: k=kyx und g=gxy
Kürzungsregel ergibt: 1=yx und 1=xy
d.h. $x,y \in E(M)$

Ergebnis: In einem kommutativen Monoid mit Kürzungsregel unterscheiden sich ggT's nur um Einheiten: ggT(a,b)=gE(M)

Bemerkung: In N nur $1 \in E(N)$
In Z nur $-1,1 \in E(Z)$

[Beispiel mit Kürzungsregel: Intergritätsbereiche (d.h. komm. R-m-1 ohne Nullteiler.): Z,K[x]]

F:Dasselbe ohne Kürzungsregel? Gegenbeispiel? Ring mit Nullteiler?
(z.B. Matritzen, Innere direkte Summe zweier Ringe)

F.7.1: Gilt A6 für $a,b,Q_i,r_i \in R$: kommutativer R-m-1?

A.7.1: Durch die Wahl der $Q_i \in R$ sind die $r_{i+1} \in R$ festgelegt!

[Bemerkung: Im üblichen EA für IN werden die Q_i so gewählt, dass $0 \leq r_{i+1} < r_i$ ist. (D.h. EA bricht ab.)
Für den EA in IR ist im Fall: $a=\sqrt{2} \in IR$, $b=1 \in IR$, $Q_i \in IN$, $0 \leq r_{i+1} < r_i \in IR$ der EA nicht abbrechend.]

F8:Wann bricht der EA ab?

F9: Betrachte 1.Schema mit $a,b,Q_0,Q_1,Q_2,...,Q_n$. (für festes n)
Betrachte 2.Schema mit $a',b',Q_0,Q_1,Q_2,...,Q_n$ aber $r_{n+1}=0$ (für festes n)

F.9.1: Gibt es solche a',b'∈R? Wie errechnen sich "diese"?

A.9.1:Wenn r_n vorgegeben, so a',b' eindeutig bestimmt (errechenbar von unten her).

F.9.2:Formel?

F.9.3:Wie ändern sich a',b' bei Änderung von r_n? Was bleibt invariant bei Änderung von r_n? Der Quotient a'/b'?

A.9.2:Antwort-Versuche

1)$r_{-1}-Q_0r_0=r_1$, $a'/b'=r_{-1}/r_0=Q_0+r_1/r_0=Q_0+1/(r_0/r_1)=Q_0+1/(Q_1+1/(r_1/r_2))$
$r_0-Q_1r_1=r_2$, $r_o/r_1=Q_1+r_2/r_1=Q_1+1/(r_1/r_2)$
$r_1-Q_2r_2=r_3$, $r_1/r_2=Q_2+r_3/r_2=Q_2+1/(r_2/r_3)$
...

2)F1 wird (wohl) mit Ja beantwortet. Also gilt $0=r_{n+1}=x_{n+1}a'+y_{n+1}b'$ für dieselben x_i,y_i ($i\leq n+1$) wie für (a,b). D.h. $a'/b'=-y_{n+1}/x_{n+1}$.

Zur vorangehenden Stunde (09.12.03),
zur nächsten Stunde (12.12.03),
zur Protokollübersicht.

Elementare Zahlentheorie

Protokoll der Sitzung vom 16.12.

von Sebastian Mohr

Euklidischer Algorithmus (EA): Schema und Durchführung
Fragen:
F10: Wenn $r_{n+1} = 0$ ist, ist dann x_{n+1} ? 0?
F11: Ist **Z** Lösungsmenge von $g = xa + yb$?
F12:Haben x_i und y_i die gleichen Vorzeichen?
F13: Sind alle Paare (x_i, y_i) teilerfremd ?
F14: Konvergiert die Folge A_2, A_3... gegen a/b ?

A13: Ja, da die Determinante immer gleich $[(x_i, y_i),(x_{i+1}, y_{i+1})]_{(2x2)}$ +- 1 ist.

zu F10 und F12: F10': Wie "wachsen" die $|x_i|$, $|y_i|$ mit i?
(Die Determinationsformel lautet: $x_{i-1} - Q_i x_i = x_{i+1}$, für y_{i+1} analog.)

i	**x**	**y**
-1	1	-0
0	-0	1
1	1	$-Q_0$
2	$-Q_1$	$1+Q_0Q_1$

Betrachte den EA für a,b ? **N** mit Q_i *isin* **N** (üblicher EA).
Zu zeigen ist, dass x_i und x_{i+1} verschiedene Vorzeichen haben.
Induktions Verankerung:x_i und x_{i+1} haben verschiedene Vorzeichen.
Induktion: x_{k+1} und x_{k+2} sind zu vergleichen.
Es ergibt sich aus deer Definition: $x_k - Q_{k+1}x_{k+1} = x_{k+2}$ *und* $x_{k-1} - Q_k x_k = x_{k+1}$
Da die Vorrausetzung nicht ausreicht muß sie verschärft werden:
Es sei $x_i > 0$ für $i \geq 1$ ungerade und $x_i < 0$ für $i \geq 2$ gerade.
Es folgt, dass wenn k ungerade ist, $k+1$ gerade ist.
$x_{k+1} = x_{k-1} - Q_k x_k < 0$ da x_{k-1} kleiner und Q_k und x_k größer 0 sind.
Analog folgt, dass wenn k gerade ist, ist $k+1$ ungerade.||

Folgerung:
$|x_{k+1}| = |x_{k-1}| + Q_k * |x_k| \geq |x_{k-1}| + |x_k| = f_{k+1}$.
"Alle $Q_i = 1$" ergibt:

-1	1	0
0	0	1
1	1	Q_0
2	1	$1+Q_0Q_1$
3	2	

4 3
5 5

Wobei die Fibonacci- Folge so definiert ist: $f_1 := 1$, $f_0 := 0$, $f_{i-1} + f_i =: f_{i+1}$.

A10:
x_k ist größer 0 für alle $k \geq 1$. Analog folgt für die y_i : Mit dem gleichen Beweis ergibt sich: $y_i < 0$ für $i \geq 1$ ungerade und $y_i > 0$ für $i \geq 0$ gerade. Die Folgerung lautet: $|y_{k+1}| = |y_{k+1}| + Q_k|y_k| \geq |y_{k-1}| + |y_k| = f_{k+2}$.

zu F11:

A)

Zum allgemeinen Teil betrachtet man die Lösungsmenge einer linearen Gleichung über **Z** mit zwei Unbekannten (aus **Z**).
Mit $ax + by = c$ (a, b, c aus **Z** gegeben)
und gesucht **L**:= {(x, y) ? **Z x Z** | $ax + by = c$ }.
A11: Betrachte zuerst **H** (homogen): H:= {(x, y) ? **Z xZ** | $ax + by = 0$ }.
H ist ein **Z**-Teilmodul von $\mathbf{Z}^{1x2}$.
Im Fall $(a, b) = (0, 0)$ ist $\mathbf{H} = \mathbf{Z}_{1x2}$.
Im Fall(a, b) ? (0, 0) ergibt sich ($-b, a$) ? **H** \ (0, 0), es folgt ? **H**, es folgt f *($-b/g, a/g$) ? **H**.

Somit ergibt sich $\mathbf{Z}^*(-b/g, a/g) \leq \mathbf{H}$.
Wenn b ? 0 ist, so folgt für (x, y) ? **H**: $y = -a/b*x = -a/g \,/\, b/g \,*x$ in **Q**.

Frage: Für welche x ? **Z** ist y ? **Z** ?
Aus (b/g)*y = (a/g)*x (in Z) folgt (mit (b/g) und (a/g) teilerfremd):
$x = (b/g)*f$ und $y = (a/g)*ß = -(a/g)*f$ (f und ß aus **Z**).
Also folgt: -f = ß.
Somit ergibt sich: $(x,y) = (b/g, a/g)*f$.

Das Fazit lautet: $\mathbf{H} = \mathbf{Z}^*(-b/g, a/g) = \mathbf{Z}^*(b/g, -a/g)$.

Zusatzfrage: Existieren weitere (x_0, y_0) mit $\mathbf{H} = \mathbf{Z}^*(x_0, y_0)$? NEIN!

B)

Anwendung auf den ggT mit $g = ax_n + by_n$ bei üblichen EA ($x_{n+1} = 0$).
Wenn der übliche EA mit $r_{n+1} = 0$ endet, ist $r_n = g$ ein ggT von (a, b).
Also sind $r_n : g = ax_n + by_n$ und (x_{n+1}, y_{n+1}) ? H : $0 = ax + by$ teilerfremd.
Daraus folgt: $(x_n, y_n) = (-b/g, a/g)$ oder $(b/g, -a/g)$.
Nach F10 und F12 ist $|x_{n+1}| > |x_n|$ und $|y_{n+1}| > |y_n|$. Also berechnet der Algorithmus die optimale Lösung.
$\mathbf{L} = \mathbf{H} + (\underline{x}, \underline{y})$ für jede beliebige (spezielle) Lösung in **L**.
Beweis:
≥
Gilt für (x', y') ? **H** $(\underline{x}+x', \underline{y}+y')$? **L** ?

$a*(\underline{x} + x') + b*(\underline{y} + y') = (a\underline{x} + b\underline{y}) + (ax' + by') = c + 0 = c$.
$\leq$ selbst... ||.

zu F14:

Gegeben seien ein *ä* (> 0) ? **R** []. Der übliche EA breche nicht ab, also *ä* ? **R\ Q**.
Für a:= *ä* und b:= 1 mache EA mi $\mathbf{Q_i}$? **N**.

Definition. $A = - y_{n+1} / x_{n+1}$.

[Motivation: Vergleiche EA für *a,b,ä* mit EA für $\underline{ä}$, $\underline{a} = \underline{ä}$, $\underline{b} = 1$, wobei die $\mathbf{Q}_i$ bis $i < n$ (aber $\underline{r}_{n+1} = 0$)gleich sind. Also sind $\underline{x}_i = x_i$ und $\underline{y}_i = y_i$, für $i \leq n+1$.

Jetzt ist $\underline{r}_i = \underline{a}x_i + \underline{b}y_i$, wie immer für $i \leq$ n+1, insbesondere $i = n+1$ und $0 = \underline{a}x_i + \underline{b}y_i$,
also $\underline{a}/\underline{b} = -\underline{y}_{n+1} / -\underline{x}_{n+1} = \underline{ä} = - y_{n+1} / x_{n+1} =: A_n$.]

Elementare Zahlentheorie 18.12.2003 (AZ)

Zur vorangehenden Stunde (16.12.03),
zur nächsten Stunde (19.12.03),
zur Protokollübersicht.

§ 8 Pythagoräische Zahlentripel

[Bemerkung: Früher schrieb man wohl "pythagor **e** isch".]

I. Geschichte, Geometrie, Arithmetik

Definition 1: Ein PZT ist ein Tripel *(x, y, z)* aus **drei natürlichen Zahlen** *x, y, z,* die die Gleichung $x^2 + y^2 = z^2$ erfüllen.

Beispiel: (3, 4, 5) ist ein PZT, da 9 + 16 = 25 ist.

Man kann ein PZT auf zwei Weisen betrachten:

- einerseits kann man es algebraisch deuten: und zwar als natürliches Lösungstripel der Gleichung $x^2 + y^2 = z^2$;

- andererseits kann man es geometrisch deuten als pythagoreisches, d.h. rechtwinkliges Dreieck, kurz PD, mit den Katheten x und y und der Hypotenuse z.

Zur Geschichte:

Man weiß heute, dass schon vor ca. 4000 Jahren pythagoräische Zahlentripel bekannt waren und zwar bei den Babyloniern, also rund 1500 Jahre vor Pythagoras. Das älteste bekannte Zeugnis ist die rund 3800 Jahre alte so genannte babylonische Keilschrifttafel Plimpton 322 (Babylonier lebten in Mesopotamien – heutiger Irak- eine der ersten Hochkulturen). Sie wurde in der ersten Hälfte des 19. Jh. im Irak ausgegraben, und ihre erste Interpretation stammt aus dem Jahre 1935. Auf dieser Tafel sind 15 PZT aufgeschrieben, u.a.

(6480, 4961, 8161) und (13500, 12709, 18541). Dabei fällt auf, dass 8161 und 18541 Primzahlen sind. Da diese Tripel mit Sicherheit nicht durch bloßes Ausprobieren gefunden wurden, stellt sich nun die Frage 1), wie die Babylonier sie gefunden haben, und 2), wie man heute solche Tripel finden kann.

(Zur Geschichte: QUELLE:
http://hischer.de/uds/forsch/vortrag/hischer/ringvl02/funkbegr.pdf)

Zu 2):

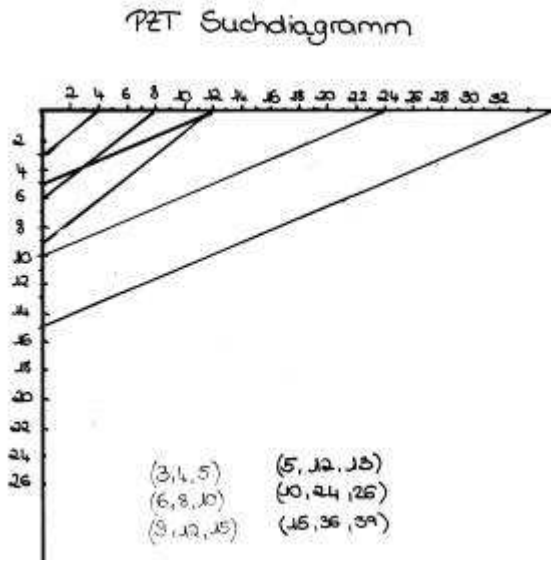
2.1) Anwendungsbeispiel für die Schule

Knotenschnur:

Man stellt den Schülern ein Brett und ein Seil mit zwölf Knoten in regelmäßigen Abständen zur Verfügung. Nun stellt man den Schülern die Aufgabe, auf dem Brett mit der Schnur ein PZT zu konstruieren. So entdecken die Schüler selbst, wie ein PZT entsteht. Bei zwölf Knoten gibt es dabei genau eine Möglichkeit.

2.2) Anwendungsbeispiel

PZT-Suchdiagramm:



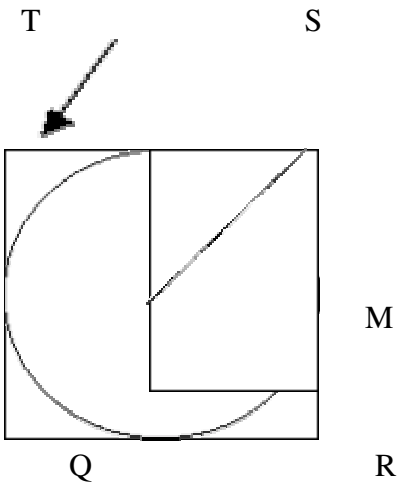
In diesem Diagramm kann man mit Hilfe eines Lineals verschieden PZT finden. Dabei stellt man fest, dass man die PZT in Gruppen einteilen kann, wobei jeweils die Hypotenusen der Mitglieder einer Gruppe parallel sind. Das heißt also, dass die algebraische Operation „Multiplikation des Tripels oder der Gleichung mit einer natürlichen Zahl *k*“ geometrisch eine zentrische Streckung der Seitenlängen um das Zentrum C bedeutet.

Definition 2: Ein PZT *(x, y, z)* mit paarweise teilerfremden *x, y, z* heißt primitives PZT.

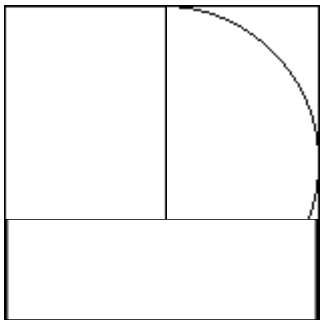
Daraus folgt, dass man den kleinsten Vertreter jeder Gruppe von PZT primitiv nennt.

2.3) Geometrische Konstruktion:

Ein Quadrat mit seinem Inkreis



Um zum zweiten Tripel zu kommen benötigt man die Werte des ersten.



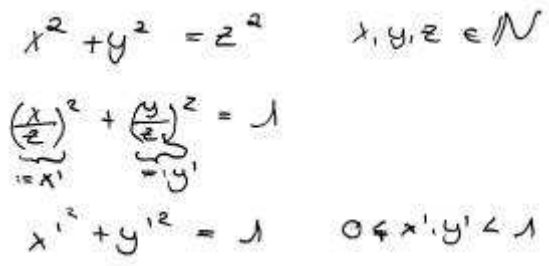
Man verbindet den linken unteren Eckpunkt des äußeren Quadrates mit Q und erhält den Schnittpunkt M . Dann kann man das Tripel ablesen.

Dabei sind die Verhältnisse immer QR = 6/5 *r* und QS = 8/5 *r* (*r* Radius des Kreises).

Bei iterariver Fortsetzung der Reihe erhält man alle primitiven PZT.

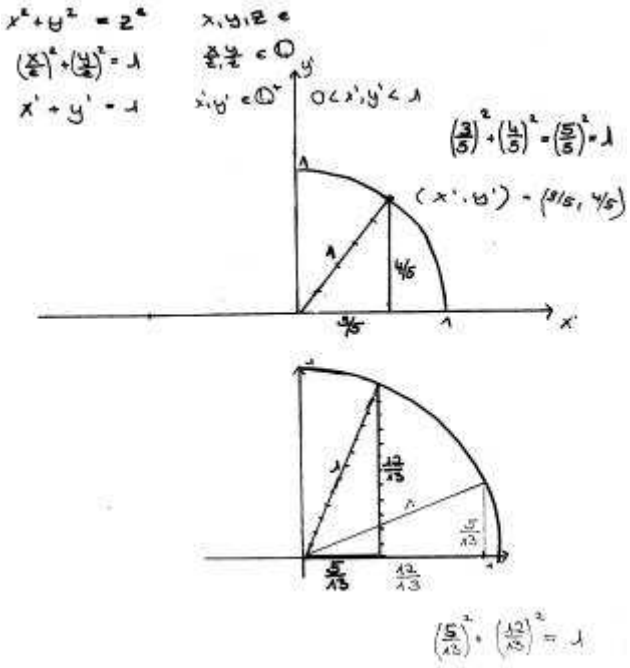
2.4) **Einheitskreis**

Zunächst stellt man die Anfangsgleichung des PZT so um, dass man eine Kreisgleichung für einen Einheitskreis erhält.



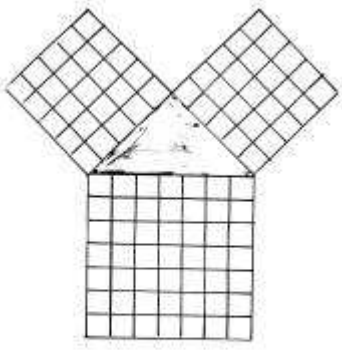
Dann kann man Werte für $x´$ und $y´$ berechnen. Diese Gleichung hat als Graphen den Viertelskreisbogen des Einheitskreises (ohne Endpunkte).

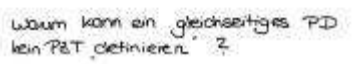
Genau die Punkte auf dem Viertelskreisbogen mit *rationalen* Koordinaten definieren ein PZT.



Wenn man so ausreichend viele Beispiele gefunden hat und diese alle in ein Achsenkreuz einträgt, erhält man einen Kreis. Diese Tatsache hat einen hohen architektonischen Wert. ...

Frage: Warum kann ein gleichseitiges rechtwinkliges Dreieck mit Kathetenlänge x und Hypothenusenlänge y kein PZT definieren?





Als Ausgangsgleichung hat man $x^2 + x^2 = y^2$. Stellt man diese Gleichung um, so erhält man $2^{1/2}x = y$. Daraus folgt, dass y keine rationale Zahl ist, also kein PZT definieren kann.

Frage: Wie kann man ein PZT algebraisch entwickeln?

Voraussetzung: eine Kathetenlänge ist gerade (x) und eine ist ungerade (y).

Zu zeigen: Es können nicht beide ungerade sein.

Beweis: Angenommen, x und y sind ungerade.

$(2n - 1)^2 + (2m - 1)^2 = (2k)^2$

$4n^2 - 4n + 1 + 4m^2 - 4m + 1 = 4k^2$

$4(n^2 - n + m^2 - m) + 2 = 4k^2$

$2(n^2 - n + m^2 - m) + 1 = 2k$

ungerade gerade

Widerspruch!

Alternativbeweis: Angenommen, x und y sind ungerade.

$(2n + 1)^2 + (2m + 1)^2 = (2k)^2$

$4n^2 + 4m + 1 + 4m^2 + 4m + 1 = 4k^2$

$n^2 + n + m^2 + m + 0{,}5 = k^2$

nicht in **N** in **N** Widerspruch!

Zu zeigen: x und y sind paritätsverschieden.

$x^2 + y^2 = z^2$ (1)

$y^2 = z^2 - x^2$ (2)

$y^2 = (z - x)(z + x)$ (3)

$(z - x)$ und $(z + x)$ sind beide gerade, also

$y^2/4 = (z + x)/2 * (z - x)/2$ (4)

Quadratzahl teilerfremd teilerfremd

Zu zeigen: $(z + x)/2$ und $(z – x)/2$ sind teilerfremd.

Beweis: Angenommen, $g \mid (z + x)/2$ und $g \mid (z – x)/2$.

Daraus folgt $g \mid (z + x + z – x)/2$ und $g \mid (z + x – z + x)$.

also $g \mid z$ und $g \mid x$.

Daraus folgt $g \mid y$ (kein primitives PZT).

Frage: Wie berechnet man nun die Menge aller primitiven PZT?

Antwort:

$(y/2)^2 = (z + x)/2 * (z – x)/2$

$c^2 = a^2 * b^2$

Dann ist $z + x = 2a^2$ und $z – x = 2b^2$.

Daraus folgt: $x = 2a^2 - z$ und $z = 2b^2 + x$,

also $x = a^2 - b^2$ und $z = a^2 + b^2$.

Aus (2) folgt dann $y^2 = (a^2 + b^2)^2 - (a^2 - b^2)^2 = 4a^2b^2$,

$y = 2ab$.

Behauptung:

Daraus folgt dann: Die Menge aller primitiven PZT ist

$$L = \{(x, y, z) \text{ in } \mathbf{Z}^3 \mid (x, y, z) = (a^2 - b^2, 2ab, a^2 + b^2) ; a, b \text{ in } \mathbf{N},$$

$$a > b, ggT(a, b) = 1, a \text{ und } b \text{ paritätsverschieden}\}.$$

Beweis: „ --> “ *gezeigt.*

„ <-- “ *muss man zeigen, und dann sieht man: es stimmt!*

Probe: Wie findet man jetzt Beispiele?

Beispiele sind: (15, 8, 17), (88, 105, 137), (2244, 1700, 2756), (7, 24, 25).

Zur vorangehenden Stunde (16.12.03),

Elementare Zahlentheorie WS 03/04
Protokoll vom Fr., 19.12.03 (IS).

Zur vorangehenden Stunde (18.12.03),
zur nächsten Stunde (08.01.04),
zur Protokollübersicht.

3. Methode zur Berechnung der Pythagoräischen Zahlentripel (1628):

Satz: Es sei x eine beliebig angenommene Kathete eines rechtwinkligen Dreiecks mit Seiten(längen) x, y, z, so dass $x^2 + y^2 = z^2$ und x, $y, z \in \mathbf{N}$. Dann gibt es einen Teiler $d \in \mathbf{N}$ von x^2, für den gilt: $y = \frac{1}{2} * (x^2/d - d)$ und $z = y + d$.
Bew. : $y + d = z$, daraus folgt $d = z - y$. Also gilt: $y = \frac{1}{2} * (x^2/(z - y) - (z - y))$. Und daraus folgt $y = y$. /
[Ist das ein Beweis? US]

F1. Wie kommt man auf diese Idee?
A1. Man stellt sich d als Differenz zwischen der Hypotenuse und einer Kathete vor. Also sei $z = y + d$. Bestimme nun y aus $x^2 + y^2 = z^2$.
Also gilt: $x^2 + y^2 = (y + d)^2$, und daraus folgt: $y = \frac{1}{2} * (x^2/d - d)$. /

F2. Findet man so alle Pythagoräischen Zahlentripel?
A2. Aus $y = \frac{1}{2} * (x^2/d - d)$ folgt: $(2y + d) * d = x^2$, also ist d Teiler von x^2. Außerdem sind x, y, z und $d \in \mathbf{N}$, also findet man mit "dieser Methode" alle Pythagoräischen Zahlentripel.
[Gemeint ist wohl:

- Wähle x in $\mathbf{N}$.
- Für jeden Teiler d von x^2 prüfe, ob $(x^2/d - d)$ gerade ist, und setze gegebenenfalls $y = \frac{1}{2} * (x^2/d - d)$.
  Dann ist $(x, y, y + d)$ ein pyth. Zahlentripel.

(US)]

Wir haben in den Vorlesungen also drei verschiedene Methoden kennen gelernt, um alle Tripel ausfindig zu machen: Diese waren eine Parametrisierung, eine geometrische Vorstellung und eine experimentelle Methode ohne explizite Formel.
Als **Fazit** lässt sich sagen, dass es (noch) viele (weitere) Möglichkeiten gibt, um sich den Pythagoräischen Zahlentripeln zu nähern.

Zur vorangehenden Stunde (18.12.03),
zur nächsten Stunde (08.01.04),
zur Protokollübersicht.

Elementare Zahlentheorie WS 2003 / 2004

Zur vorangehenden Stunde (19.12.03),
zur nächsten Stunde (09.01.04),
zur Protokollübersicht.

Stundenprotokoll 08.01.2004 (MH)
[Das Protokoll ist noch nicht redigiert.]

- **Begrüßung**

- **Einstieg**

  Als Wiedereinstieg nach den Ferien, wird erwähnt, dass es in unserer Vorlesung um zweierlei Dinge geht: Erstens um Mathematik und zweitens um die Didaktik der Mathematik. Außerdem wird besonder Wert darauf gelegt, dass auch die Mathematik wichtig ist. Insbesondere ist die Mathematik eine ehrliche Wissenschaft. Man kann in der Mathematik nichts verschweigen und muss alle Argumente in Betracht ziehen. Man muss alles genau aufschreiben und gut hinsehen, ob auch wirklich alles erwähnt wurde, oder ob ein weggelassenes Argument das Ergebnis verändern würde und eine Tatsache übersehen wurde.

  Diese Erkenntnis ist vor allem auch in der Schule wichtig. Jeder macht mal Fehler, aber es ist falsch den Schülern etwas „vorzuflunkern".

- **Themeneinstieg**

  Wir beschäftigen uns mit Pythagoräischen Zahlentripeln (PZT). Wir kennen bereits eine Möglichkeit, diese Zahlen zu finden. Jedoch interessiert es uns, mehrere Zugänge zu ein und demselben Thema zu finden.

  Auch Schüler müssen lernen, eine Aufgabe nicht nur mit einer einzigen Regel zu lösen. Es gibt fast immer verschiedene Lösungswege.

- **Fragen**

  Bestimmung aller pythagoräischen Tripel (x, y, z) aus $\mathbf{N}^3$ mit $x^2 + y^2 = z^2$ und primitives PZT (PPZT) ?

  (Man könnte auch die Null oder die Ganzen Zahlen statt der Natürlichen Zahlen nehmen, diese Erweiterung würde jedoch nichts wesentlich Neues bringen und wir können uns auf die Natürlichen Zahlen beschränken).

- **Planen**

  a) Algebraischer Zugang (erledigt)

  b) Geometrischer Zugang (heute)

c) Elementarer Zugang (nächste Vorlesung)

d) Gruppentheoretischer Zugang (nächste Woche)

Dabei ist jeweils wichtig:

I) Analyse

II) Konstruktion

- **Schreiben**

Zu b) Geometrischer Zugang:

- Idee: „Pythagoräische Zahlentripel führen auf rationale Kreispunkte":

$x^2 + y^2 = z^2$ ---> $(x/z)^2 + (y/z)^2 = 1$

Mit $(x/z) = x'$ und $(y/z) = y'$,

wobei (x', y') Koordinaten eines Kreispunktes sind.

- **Plan:**

1) Beziehung zwischen PZT und rationalern Kreispunkten formalisieren und explizieren.

2) Mit Zusatz-Idee „die PZT" (primitiv) bestimmen.

- **Schreiben:**

Zu 1) *Bijektion zwischen zwei Mengen herstellen.*

i) Von PZT zu rationalen Einheitspunkten:

Zu (x, y, z) aus PZT bilde $(x', y') = (x/z, y/z)$ aus Rationaler Einheitskreispunkt (REP)

REP := { (x', y') aus $\mathbf{Q}^2$ mit $x'^2 + y'^2 = 1$; $x', y' > 0$}

κ: PZT ---> REP

(keine Bijektion, da OZT, die sich nur um Faktor λ unterscheiden, dasselbe Bild erreichen).

κ': PPZT ---> REP

Bild κ = Bild κ'

- **Frage:**

  Ist κ' injektiv, surjektiv ?

- **Schreiben:**

  κ' injektiv: (x, y, z), ($\underline{x}$, $\underline{y}$, $\underline{z}$) aus PPZT mit (x/z, y/z), ($\underline{x}$/$\underline{z}$, $\underline{y}$/$\underline{z}$) gegeben.

  Da x/z und $\underline{x}$/$\underline{z}$ gekürzte Brüche (primitiv), folgt: x = $\underline{x}$, z = $\underline{z}$, y = $\underline{y}$. Das bedeutet, dass κ' injektiv ist.

  ii) *Von REP nach PPZT:*

  (x', y') = (x/z, y/z) (gekürzte Brüche, tfrd.) mit $(x/z)^2 + (y/z)^2 = 1$.

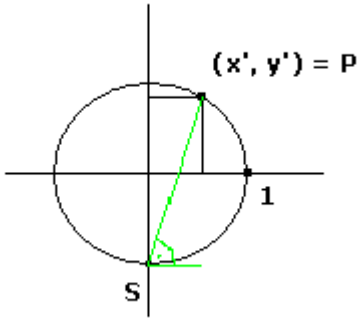
  Dies ergibt: (x, y, z) aus PPZT;

  κ' surjektiv: also ist κ' surjektiv.

- **Schreiben:**

  Zu 2) Bestimmung / Beschreibung von PPZT und REP.

[Es geht noch weiter.]



- **Analyse:**

  Es sei (x/z, y/z) = (x', y') aus REP mit $x'^2 + y'^2 = 1$.

  Gerade SP habe die Steigung s/t = (1 + y') / x' aus **Q**. Dabei ist s/t gekürzter Bruch und s > t.

  Aufgelöst:

  $y' = (s/t)\, x' - 1$

  $x'^2 + [(s/t)\, x' - 1]^2 = 1$

  $[1 + (s^2/t^2)]\, x'^2 - 2\,(s/t)\, x' = 0$

  Daraus ergibt sich durch Ausklammern:

  x' = 0 (Widerspruch zu (x', y') aus REP), oder

  $[1 + (s^2/t^2)]\, x' = 2\,(s/t)$.

  Durch Ausrechnen und Einsetzen ergibt sich schließlich:

  $x' = 2st/(s^2 + t^2) = x/z$

  $y' = (s^2 - t^2)/(s^2 + t^2) = y/z$

  für (x, y, z) aus PPZT.

  Das bedeutet:

  $2st = \lambda x$

  $s^2 + t^2 = \lambda z$

  $s^2 - t^2 = \lambda y$.

  Daraus ergibt sich ein Zwischenergebnis:

  $(2st, s^2 - t^2, s^2 + t^2) = \lambda(x, y, z)$, für ein λ aus **N**.

  $(2st/\lambda, (s^2 - t^2)/\lambda, (s^2 + t^2)/\lambda) = (x, y, z)$.

  Dann ist λ = ggT $(2st, s^2 - t^2)$, wobei ggT (s,t) = 1.

- **Konstruktion:**
- **Frage:**

  Liefern alle (s, t) aus N^2 PPZT? Welche liefern PPZT, welche PZT?

- **Schreiben:**

  $(2st)^2 + (s^2 - t^2)^2 = 4s^2t^2 + s^4 - 2s^2t^2 + t^4$

  $= s^4 + 2s^2t^2 + t^4$

  $= (s + t)^2$

  also immer pythagoräisch. Aber wann ist es aus PPZT?

- **Plan:**

  3 Fälle zu betrachten:

  A) $s \equiv 0 \equiv t \bmod 2$

  B) $s \equiv 1 \equiv t \bmod 2$

  C) $s \equiv 0, t \equiv 1 \bmod 2$, oder umgekehrt.

- **Schreiben:**

  Zu A) 2 teilt s, t : nicht zugelassen

  Zu B) 2 teilt g = ggT $(2st, s^2 - t^2, s^2 + t^2)$

  [$s = 2u + 1\ u > v \geq 0$

  $t = 2v + 1\ s > t \geq 0$

  Einsetzen in $T = (2st, s^2 - t^2, s^2 + t^2) = (2(2u+1)(2v+1), 4(u-v)(u+v+1), 4(u^2+v^2+u+v)+2)$,

  wobei $(u-v) =: s'$ und $(u + v + 1) =: t'$.

  Dividiere durch 2:

  $\frac{1}{2}\ T = (s'^2 - t'^2, 2s't', s'^2 + t'^2)$

s' + t' = (u+v+1) + (u – v) = 2u + 1 = s (ungerade)

---> Fall C) für (s', t')**]**.

Zu C) Es sei $s > t \geq 1$, ggT (s, t) = 1, $s \equiv t \bmod 2$

Dann ist $(2st, s^2 - t^2, s^2 + t^2)$ primitiv.

Es sei:

X:= 2st Y:= $s^2 - t^2$ Z:= $s^2 + t^2$.

Beweis:

g : = ggT (2st, $s^2 - t^2$), 2 teilt g nicht;

g teilt Y + Z = $2s^2$

g teilt -Y + Z = $2t^2$

Daraus ergibt sich:

g teilt s^2, t^2, da diese teilerfremd sind, folgt: g = 1.

Das bedeutet, dass C) automatisch primitiv ist.

- **Analyse-Fazit:**

  PPZT sind von der Form $(2st, s^2 - t^2, s^2 + t^2)$ oder $(s'^2 - t'^2, 2s't', s'^2 + t'^2)$,

  wobei $s > t \geq 1$, ggT (s, t) = 1.

Zur vorangehenden Stunde (19.12.03),
zur nächsten Stunde (09.01.04),
zur Protokollübersicht.

Elementare Zahlentheorie WS 2003/04

Protokoll vom 09.01.04 (AE)

Zur vorangehenden Stunde (08.01.04),
zur nächsten Stunde (13.01.04),
zur Protokollübersicht.

Thema der Stunde: Ein elementarer Zugang zu pythagoreischen Zahlentripeln (Forts. von § 8)

II Aufgabe: Bestimme **alle PPZT** (primitive pythagoreische Zahlentripel) *(x, y, z)*, wobei *x, y, z* natürliche Zahlen sind.

Ansatz:

1. Suche Tripel mit $z = x + 1$ (wie zum Beispiel *(4, 3, 5)*).
2. Suche Tripel mit $z = x + 2$.
3. Suche Tripel mit $z = x + 3$.
4. Suche Tripel mit $z = x + 4$.
5. Suche Tripel mit $z = x + 5$.
6. Suche Tripel mit $z = x + 6$.
7. ....
8. Suche Tripel mit $z = x + p$, p Primzahl.
9. Suche Tripel mit $z = x + k$, k natürliche Zahl.

Ergebnisse:

1. Alle Tripel mit $z = x + 1$ sind von der Form $((y^2 - 1) / 2, y, (y^2 + 1) / 2)$ für *ungerades y*. Diese Darstellung wird **pythagoreische Serie** genannt.
2. Alle Tripel mit $z = x + 2$ sind von der Form $((y^2 - 4) / 4, y, (y^2 + 4) / 4)$ für *gerades y*. Diese Darstellung wird **platonische Serie** genannt.
3. Alle Tripel mit $z = x + 3$ sind von der Form $(3 (y^2 - 1) / 2, 3y, 3(y^2 + 1) / 2) = 3((y^2 - 1) / 2, y, (y^2 + 1) / 2)$. PZTs von dieser Form sind nicht primitiv, wir bezeichnen die Darstellung als **3mal pythagoreische Serie**. Wir haben also keine neuen (primitiven) Lösungen gefunden.
4. Alle Tripel mit $z = x + 4$ sind von der Form $2((y^2 - 4) / 4, y, (y^2 + 4) / 4)$. PZTs von dieser Form sind nicht primitiv, wir bezeichnen die Darstellung als **2mal platonische Serie**. Wir haben also keine neuen Lösungen gefunden.
5. Alle Tripel mit $z = x + 5$ sind von der Form $5((y^2 - 1) / 2, y, (y^2 + 1) / 2)$. PZTs von dieser Form sind nicht primitiv, wir bezeichnen die Darstellung als **5mal pythagoreische Serie**. Wir haben also keine neuen Lösungen gefunden.
6. Alle Tripel mit $z = x + 6$ sind von der Form $6((y^2 - 4) / 4, y, (y^2 + 4) / 4)$. PZTs von dieser Form sind nicht primitiv, wir bezeichnen die Darstellung als **6mal platonische Serie**. Wir haben also keine neuen Lösungen gefunden.
7. .... Vorläufiges Fazit: Offenbar findet man keine neuen Lösungen mehr. Alle Lösungen sind bisher von pythagoreischer oder platonischer Form.

8. Alle Tripel mit $z = x + p$ (p Primzahl) sind von der Form $p((y^2 - 1) / 2, y, (y^2 + 1) / 2)$. Es handelt sich also um die **p**mal platonische Serie.

   Beweis: Löse zunächst die Gleichung $x^2 + y^2 = (x + p)^2$ nach x auf. Man erhält $x = (y^2 - p^2) / (2p)$. Es gilt also: $2p$ teilt $y^2 - p^2$,
   insbesondere p teilt $y^2 - p^2$ und p teilt y^2 . * Hieraus folgt, da p Primzahl ist, dass p auch y teilt. y ist also von der Form $y = pt$, t natürliche Zahl. Es gilt also:

$$\boldsymbol{x} = (p^2t^2 - p^2) / (2p) = p (t^2 - 1) / 2,$$
$$\boldsymbol{y} = pt,$$
$$\boldsymbol{z} = x + p = p (t^2+1) / 2.$$

9. Sind alle Tripel mit $z = x + k$ (k beliebige natürliche Zahl) entweder von pythagoreischer oder platonischer Form?

   Nachweisversuch: (Der Anfang verläuft bis * analog zu 8.) Löse zunächst die Gleichung $x^2 + y^2 = (x + k)^2$ nach x auf. Man erhält

$$x = (y^2 - k^2) / (2k).$$

   Also gilt: $2k$ teilt $y^2 - k^2$, also k teilt $y^2 - k^2$ und y^2. Wir betrachten die Primfaktorzerlegung von k und stellen fest, dass sich k in einen quadratischen und einen quadratfreien Teil zerlegen lässt:

$$k = k_1^2 k_2, \text{ wobei } k_1, k_2 \text{ natürliche Zahlen sind und } k_2 \text{ quadratfrei ist.}$$

   Also folgt: $k_1 k_2$ teilt y und y lässt sich als

$$\mathbf{y} = k_1 k_2 t \text{ mit einer natürlichen Zahl } t$$

   darstellen. Für x folgt:

$$\boldsymbol{x} = (y^2 - k^2) / (2k) = \ldots = k_2 (t^2 - k_1^2) / 2.$$

   Für z folgt:

$$\boldsymbol{z} = k_2(t^2 + k_1^2) / 2.$$

   Insgesamt haben wir
   $(x, y, z) = (k_2(t^2 - k_1^2) / 2, t k_1, (t^2 + k_1^2) / 2)$ für gerade k_2 (wir nennen dies die **k_2-pythagoreische Serie**) und
   ?? $(x, y, z) = (k_2 (t^2 - k_1^2), 2tk_1, t^2 + k_1^2)$ für ungerade k_2 (wir nennen dies die **k_2- platonische Serie**).
   Hier erhält man also für geeignete k_2 doch neue PZT.

Zur vorangehenden Stunde (08.01.04),
zur nächsten Stunde (13.01.04),
zur Protokollübersicht.

Elementare Zahlentheorie WS 2003/04

Stundenprotokoll der Sitzung vom 13.11.04 (SM)
[Das Protokoll ist noch nicht redigiert.]

Zur vorangehenden Stunde (09.01.04),
zur nächsten Stunde (15.01.04),
zur Protokollübersicht.

Thema (Vortrag ST zu § 8): Eine gruppentheoretische Beschreibung der PPZT.

Definition 1: Es sei $M \in \{\mathbf{N}, \mathbf{N_0}, \mathbf{Z}\}$

a) Eine Matrix $[a, b, c] \in M^{1x3}$ heißt M-phytagoreisches Zahlentripel, wenn $a^2 + b^2 = c^2$ ist.
b) Ein Pythagoreisches Zahlentripel (PZT) heißt primitiv (pPZT), wenn $(a, b, c) \in E(M)$.
Aufgabe: Bestimme alle pPZT !
Idee: Konstruktion aus einem Element.
[Menge aller pPZT := P_M]

Es sei $[a, b, c] \in P_Z$, dann gilt:

a) $[b, a, c] \in P_Z$,

b) Dann ist $T \in P_Z$ wobei $T \in \{[e_a a, e_b b, e_c c] | e_a, e_b, e_c \in \{+-1\}\}$.

Beweis:
a) Kommutativität in **Z** b) $(e_a a)^2 + (e_b b)^2 = (e_c c)^2$

Ansatz:
a) $(t - a)^2 + (t - b)^2 = (t + c)^2$
b) $(t + a)^2 + (t + b)^2 = (2t - c)^2$</sup>
jeweils für beliebige $T \in \mathbf{Z}$.

Es folgt für

a) $t = 0$ oder $t = 2(a + b + c)$,

b)$t = 0$ oder $t = a + b + 2c$.

Satz 1:>

Es sei $[a, b, c] \in P_Z$. Dann ist auch $[a+2b+2c, 2a+b+2c, 2a+2b+3c] \in P_Z$.

Beweis:

i) *T* pythagoreisch. ok

ii) *T* primitiv

Es ist $[a, b, c]$ primitiv mit $g := ggT [a+ 2b + 2c , 2a + b + 2c , 2a + 2b + 3c]$, somit gilt $g | a+ 2b + 2c , g | 2a + b + 2c , g | 2a + 2b + 3c$.

Dann gilt: $g | -a+b, g | b+c, g | a+c$ und

$g | a+ 2b + 2c + 2(2a + b + 2c) - 2(2a + 2b + 3c) = a$

$g | 2(a+ 2b + 2c) + (2a + b + 2c) - 2(2a + 2b + 3c) = b$.

Dann ist g isin; $\{+-1\}$ also $T \in P_Z$.

Definition 2: Die von { } erzeugte Untergruppe von GL (3**Z**), wobei die Matrizen wie folgt bestimmt sind

P:=

0 1 0
1 0 0

0 0 1

M_1 = [

-1 0 0

0 1 0

0 0 1

M_2 =

1 0 0

0 -1 0

0 0 1

M_3 =

1 0 0

0 1 0

0 0 -1

A =

1 2 2

2 1 2

2 2 3

heißt bei Sebastian Thomas Z-pythagoreische Gruppe $G < GL(3, \mathbf{Z})$.

Definition 3: Wir definieren Folgende Operatinen von G_z auf P_z:

$*A =: (T \to TA), P_Z \to P_Z$ für ein $A \in G_Z$

Frage: Ist P_Z eine G_z-Menge?

i) $(T*A)*B$ wobei $A, B \in P_Z$, ii) $T*E = T$.

Lemma: P_Z ist eine G_z. Beweis ok.

Fragen: 1. Eigenschaften von G_z (Ordung...)?

2. Isomorphietypen ?

3. Andere Gruppen ?

Definition 4: zu 1)Es sind $B := M_1 A$, $C := M_2 A$ und $D := M_1 M_2 A$ mit den Ordnungen:

o(P) = 2

o $(M_i)A$ = 2, I ? {1,2,3}

o(A), o(B), o(C), o(D) = ?. Die Ordung von A, B, C sind wohl unendlich und o(D) = 2, zu zeigen mit vollständiger Induktion. Außerdem sei $G_{\mathbf{Z}} = < P, M_1, M_2, M_3, D >$ mit $o(G_{\mathbf{Z}} =$ unendlich)

zu 2) Mit T = [3, 4, 5] ergibt sich

T*A mit A ? $\{A, B, C, M_3 A, D, M_3 B, M_3 C, M_3 D\}$. Es ergibt sich:

T*A =	[21,20,29]
T*B =	[15,8,17]
T*C =	[5,12,17]
T*D =	[1,0,1]

$T*M_1M_2M_3A$ = [-21,-20,-29]

$T*M_1M_3A$ = [-5,-12,-13]

$T*M_2M_3A$ = [-15,-8.-17]

$T*M_3A$ = [1,0,-1]

M:= (m_1,m_2,m_3) : 1>* 2>*3> : 8 < G_z.

Vermutung: "A,B,C,D reichen aus".

Lemma: Es seien [*a,b,c*] isin; P_{N_0} und [*a',b',c'*] isin; P_{Z_0} .Dann gilt:

a) Aus [*a',b',c'*] = [*a,b,c*] * A folgt *a'*> *a, b'*> *b, c'*> *c*.

b) Aus [*a',b',c'*] = [*a,b,c*] * B folgt $a' \geq a$, $b' \geq b$, $c' \geq c$.

c) Aus [*a',b',c'*] = [*a,b,c*] * C folgt $a' \leq a$, $b' \leq b$, $c' \leq c$.

d) Aus [*a',b',c'*] = [*a,b,c*] * D folgt $|a'| \leq a$, $|b'| \leq b$, $|c'| \leq c$.

e) Aus [*a',b',c'*] = [*a,b,c*] * D und [*a,b,c*] nicht Element von {[1,0,1],[0,1,1]} folgt $a' \leq 0$ oder $b' \leq 0$.

Zur vorangehenden Stunde (09.01.04),

zur nächsten Stunde (15.01.04),

zur Protokoll übersicht.

Elementare Zahlentheorie WS 2003/04

Protokoll vom **15.01.2004** (TF) [Das Protokoll ist nicht redigiert.]
Inhalt:
Teil 1: Fortsetzung von § 8: "Gruppentheoretischer Zugang zu den PPZT".
Teil 2: Fortsetzung von § 7: Euklidischer Algorithmus (Konvergenten).

Zur vorangehenden Stunde (13.01.04),
zur nächsten Stunde (16.01.04),
zur Protokollübersicht.

Teil 1: Referat "Pythagoreische Zahlentripel"

Es stand noch ein Beweis von der letzten Veranstaltung aus:

Lemma:

Es seien $[a, b, c]$ aus P_{N_0}, $[a', b', c',]$ aus P_Z und, wie schon in der letzten Veranstaltung, die Matrizen a, $B = m_1 a$, $C = m_2 a$, und $D = m_1 m_2 a$ gegeben (siehe Protokoll vom 13.01.2004). Es gilt:

a.) Aus $[a', b', c'] = [a, b, c] * a$ folgt: $a' > a, b' > b, c' > c$.

Beweis: $a' = a + 2b + 2c > a$. (Rest analog.)

b.) Aus $[a', b', c'] = [a, b, c] * B$ folgt: $a' \geq a, b' \geq b, c' \geq c$.

Beweis: $a' = -a + 2b + 2c \geq -a + 2b + 2a = a + 2b \geq a$,

$b' \geq b$ analog,

$c' = -2a + 2b + 2c + c \geq c$.

c.) Aus $[a', b', c'] = [a, b, c] * C$ folgt: $a' \geq a, b' \geq b, c' \geq c$.

Beweis: Analog zu b.).

d.) Aus $[a', b', c'] = [a, b, c] * D$ folgt: $|a'| \leq a, |b'| \leq b, 0 \leq c' \leq c$.

Beweis: 1. Fall: $a' \geq 0$: $|a'| = -2 - 2b + 2c \leq -a - 2b + 2a + 2b = a$.

2. Fall: $a' < 0$: $|a'| = a + 2b - 2c \leq a + 2b - 2c \leq a + 2b - 2b = a$.

Analog: $|b'| \leq b$.

$c' = -2a - 2b + 3c = -2(a + b) + 3c \leq -2c + 3c = c$.

$c' = 3c - (2a + 2b) \geq 3c - (2a + 2b) = 3c - ((2a + 2b)^2)^{1/2} \geq 3c - ((2a + 2b)^2 + (2a - 2b)^2)^{1/2} = 3c - (4a^2 + 8ab + 4b^2 + 4a^2 - 8ab + 4b^2)^{1/2} = 3c - (8(a^2 + b^2))^{1/2} \geq 3c - (9c^2)^{1/2} = 0$.

e.) Aus $[a', b', c'] = [a, b, c] * D$ und $[a, b, c]$ ist nicht aus der Menge $J := \{[1, 0, 1], [0, 1, 1]\}$ folgt: $a' \leq 0$ oder $b' \leq 0$.

Beweis: Angenommen, *a´* und *b´* wären größer oder gleich 0:

*[a´´, b´´, c´´] := [a´, b´, c´] * D = [a, b, c] * D^2 = [a, b, c].*

Aus d.) folgt: $|a| = |a´´| \leq a´ \leq a$. Dann folgt: *[a´, b´, c´] = [a, b, c],* was im Widerspruch zu "*[a´, b´, c´]* ist nicht aus *J*" liegt.

Es ergibt sich die Folgerung: Die Operation **D* "verkleinert jedes *[a, b, c]* aus P_{N_0} (bis auf das Vorzeichen).

Es ergibt sich ein Reduktionsverfahren: Gegeben sei $[a_0, b_0, c_0]$ aus P_Z.

$[a_1, b_1, c_1] = [a_0, b_0, c_0] * X_0$, wobei X_o aus $<m_1, m_2, m_3> =: M$ ist, sodass $[a_1, b_1, c_1]$ aus P_{N_0} ist.

Dieser Vorgang wird iteriert: $T := [a_k, b_k, c_k] * X_k$, X_k ist aus M mit T aus der Menge *{[1, 0, 1], [0, 1, 1]} = J.*

*[1, 0, 1] = T * Y,* wobei *Y* aus *<P>* ist (P ist Permutationsmatrix). $[1, 0, 1] = [a_0, b_0, c_0] * (X_0DX_1D...X_kY)$

$[a_0, b_0, c_0] = [1, 0, 1] * (YX_k...DX_0)$.

Es ergibt sich das **Lemma**:

$a^{-1} = Dm_1m_2$, $B^{-1} = Dm_2$, $C^{-1} = Dm_1$, $D^{-1} = D$. Beweis: Selbst.

Also sind die X_i aus $<m_1, m_2>$. Daraus ergibt sich: P_Z ist transitiv. (Jedes Tripel lässt sich auf *[1, 0, 1]* zurückführen.)

Beispiel: Gegeben sei *[-51, -140, 149]* aus *PZ.*

$[51, 140, 149] = [-51, -140, 149] * m_1m_2$,

*[51, 140, 149] * D = [-33, 56, 65],*

$[33, 56, 65] = [-33, 56, 65] * m_1$,

*[33, 56, 65] * D = [-15, 8, 17],*

*[15, 8, 17] = [-15, 8, 17] * m1,*

*[15, 8, 17] * D = [3, -4, 5],*

$[3, 4, 5] = [3, -4, 5] * m_2$,

*[3, -4, 5] * D = [-1, 0, 1],*

$[1, 0, 1] = [-1, 0, 1] * m_1$.

Also ist $[1, 0, 1] = [-51, -140, 149] * (m_1 m_2 D m_1 ... D m_1)$, also $[-51, -140, 149] = [1, 0, 1] * (CBCC m_1 m_2)$.

Teil 2 der Veranstaltung war die **Fortsetzung von § 7: Der Euklidische Algorithmus (Konvergenten)**.

$0 < z$ aus IR sei gegeben. Dann sei $z : 1 = a : b = r_{-1} : r_0 := |\_z\_| + r$.

Der EA ergibt: $r_{-1} - Q_0 r_0 = r_1$ (Q_0 ist aus IN und $0 \leq r_1 < 1$).

Danach ist: $r_0 - Q_1 r_1 = r_2$ und so weiter.

(Parallel läuft der XEA mit den Startwerten $x_{-1} = 1$, $x_0 = 0$, $Y_{-1} = 0$ und $Y_0 = 1$ wie gehabt aus LAI. Ziel ist die Darstellung $r_i = x_i a + y_i b$.)

$z : 1 = a / b = Q_0 + r_1 / r_0 = Q_0 + 1 / (r_0 / r_1) = Q_0 + 1 / (Q_1 + (r_2 / r_1)) = Q_1 + 1 / (Q_1 + (1 / Q_2 + (1 / (r_2 / r_3))))$ usw.

$[Q_0, Q_1, Q_2] =: A_2$, $[Q_0, ..., Q_k] =: A_k$.

$A_k := -y_{k+1} / x_{k+1}$. Unsere Vermutung ist: A_k konvergiert gegen a / b (für k gegen unendlich). Für die rationale Zahl z bricht der EA ab mit $r_{n+1} = 0$. A_n ist a / b.

Erinnerung an **Satz 3** aus der Veranstaltung vom 12.11.2003: Die Determinante der Matrix

x_i	y_i
x_{i+1}	y_{i+1}

ist gleich $(-1)^{i+1}$. Die $A_k = -y_{k+1} / x_{k+1}$ sind gekürzt.

Satz 6 vom 16.12.2003: $x_k < 0$ für ungerade $k \geq 1$, $x_k < 0$ für gerade $k \geq 2$. $|x_{k+1}| > |x_k|$ *für* $k \geq 2$; $|x_k| \geq f_k$ $[= f_{k-2} + f_{k-1}]$. Ähnlich ist es bei den y_j.

Satz 7: $A_{k+1} - A_k = (-1)^{k+1} / x_{k+2} x_{k+1}$.

Beweis: $-y_{k+2} / x_{k+2} + y_{k+1} / x_{k+1} = (-x_{k+1} y_{k+2} + y_{k+1} x_{k+2}) / x_{k+2} x_{k+1}$ = (nach Satz 3) $-1 / x_{k+2} x_{k+1} \cdot \det H = (-1)^{k+1} / x_{k+2} x_{k+1}$, wobei $H :=$

x_{i+1}	y_{i+1}
x_{i+2}	y_{i+2}

$A_0 = -y_1 / x_1 = Q_0$ (siehe EA), $A_1 = -y_2 / x_2 = -(1 + Q_0 Q_1) / -Q_1 = 1 / Q_1 + Q_0 > Q_0 = A_0$.

Zur vorangehenden Stunde (13.01.04),
zur nächsten Stunde (16.01.04),
zur Protokollübersicht.

[Zur vorangehenden Stunde (15.01.04),
zur nächsten Stunde (20.01.04),
zur Protokollübersicht]
[Das Protokoll ist nicht redigiert.]

Stundenprotokoll zur Vorlesung Elementare Zahlentheorie vom 16.01.2004 (DB)

Fortsetzung von §7. Analyse von EA/XEA

Wir waren über die Analyse des *EA/XEA* und der Definition von Kettenbrüchen rationaler oder auch irrationaler Zahlen zu einigen Fragen gekommen.
Es ist der Bruch a/b oder $a : b$ (die wir heute als $a = a\ ,\ b = 1$ annehmen) und eine nicht abbrechenden Kettenbruch $[Q_0; Q_1, Q_2\ , Q_3,...]$.
Weiter gelte $a : b = A_n := - y_{n+1}/x_{n+1}$, wenn $r_{n+1} = 0 = x_{n+1} \cdot a + y_{n+1} \cdot b$ und $r_{i+1} - Q_i \cdot r_i = r_{i+1} < r_i$.

Frage: Konvergieren die r_i gegen 0?

Frage: Konvergieren die A_i?

Frage: Konvergieren die A_i gegen $a = a/b$, wenn $[Q_0; Q_1, Q_2\ , Q_3,...]$ die Kettenbruchentwicklung von $a : 1$ ist?

Folgenden Satz hatten wir in diesem Zusammenhang schon bewiesen:

Satz 7:
$$A_{k+2} - A_{k+1} = (-1)^{k+1}/(x_{k+2} \cdot x_{k+1})$$

Nun untersuchen wir zwei A_k die sich um zwei Stellen unterscheiden und schließen dadurch auf den nächsten Satz:

Satz 8:
$$A_{k+2} - A_k = Q_{i+2} \cdot (-1)^{k+1}/(x_{k+2} \cdot x_{k+1})$$ (mit positivem Nenner)

Beweis:
$A_{i+2} - A_i = - y_{i+3}/x_{i+3} - -y_{i+1}/x_{i+1} = (- y_{i+3}x_{i+1} + y_{i+1}x_{i+3})/(x_{i+3}x_{i+1})$
Da der Nenner bereits ist wie gewünscht betrachten wir nur noch den Zähler.
$- y_{i+3}x_{i+1} + y_{i+1}x_{i+3} = y_{i+1}(x_{i+1} - Q_{i+2}x_{i+2}) - x_{i+1}(y_{i+1} - Q_{i+2}y_{i+2}) = Q_{i+2}$
$(y_{i+2}x_{i+1} - y_{i+1}x_{i+2})$
Nun folgt mit Satz 3:
$Q_{i+2} \cdot (-1)^{i+2}$
Somit ist die Behauptung bewiesen.

Folgerung: Für Q_i*? /N* gilt:
$$A_0 < A_2 < A_4 < A_6 < ... < ... < A_7 < A_5 < A_3 < A_1 = Q_0 + 1/(Q_1)$$

Beweis: Man sieht leicht, dass diese Ungleichung für $A_0 < A_2 < A_3 < A_1$ erfüllt ist.
Aus Satz 7 und Satz 8 folgt der Rest.

Aus Satz 7 folgt die Konvergenz der A_i [$(1/x_i$ *?* $0)$ konvergiert]
Den Grenzwert nennen wir *ß? /R*.

A_i heißt Konvergente.

Es bleibt also noch zu zeigen, dass $\beta = a$ ist, d.h. $A_i < a < A_j$ für ungrade j und grade i.

Beweis: $A_0 = Q_0 < Q_0+1/(Q_0 + r_0/r_1) = a = Q_0+1/(Q_1 + 1/(r_1/r_2)) < A_1$.
Analog folgt sofort, dass $a < A_3$, $a < A_5$, $a < A_7$,...
und $a > A_2$, $a > A_4$, $a > A_8$,....

Aus diesem Ergebnis machen wir den folgenden Satz:

Satz 9: Ist $[Q_0; Q_1, Q_2,...]$ die Kettenbruchentwicklung von $0 < a \; ? \; /R$, so konvergiert die Folge der A_i gegen $\beta = a$.

Folgerung: Der Fehler der Kettenbruchentwicklung kann wie folgt abgeschätzt werden.
$|a - A_k| < |1/(x_{k+2} \cdot x_{k+i})| = 1/(x_{k+1}^2) = 1/(f_{k+2} \cdot f_{k+1})$

Frage: Konvergieren die r_i gegen 0?

Beweis: Nach dem XEA gilt: $r_k = x_k a + y_k b$ für einen Bruch a/b.
Mit $a/b = a/1$ ist $r_k = x_k a + y_k \cdot 1 \; ? \; k \; ? \; /N$.
$0 < A_i < a$ und $x_i < 0$ für alle graden $i = 2$,
$a < A_j$ und $x_j > 0$ für alle ungraden $j = 2$.

Für grade i:

$0 < r_i = x_k a + y_k < x_i A_i + y_i$ (da $x_k < 0$) $= x_i(-y_{i+1}/x_{i+1}) + y_i = 1/x_{i+1}(y_i x_{i+1} - y_{i+1} x_i) = (-1)^{i+2}/x_{i+1} = 1/x_{i+1}$.
$1/x_{i+1} \; ? \; 0$ für $i \; ? \; 8$ i gerade.
Für j ungrade Analog.

§9. Beste Approximation reeller Zahlen durch rationale Zahlen

Vorschau:
A. Konvergenten als Ultra-Approximationen.
B. Goldener Schnitt.
C. Fibonacci-Folgen.
D. Vergleich mit Heron-Verfahren.
E. Periodizität von Sonnenfinsternissen.
F. Das Planetarium von Christiaan Huygens.

Anwendungs Problem:
1. Zahnrad: Übertragungsverhältnis a ? /R (oder ? /Q für große Zähler oder Nenner) approximieren durch p/q ? /Q mit kleinem Nenner und Zähler.
2. Christian Huygens: Planetarium.
3. Nächste Sonnenfinsternis

Definition: Ein Bruch $0 < p/q \; ? \; /Q$, gekürzt, heißt eine **"distanz"-beste Approximation**, an $0 < a \; ? \; /R$, wenn $|a - p/q| < |a - u/v| \; ? \; 0 < v < q$, $u/v \; ? \; p/q$ $(u, v, p, q \; ? \; /N)$.

Definition: Ein Bruch $0 < p/q \in /Q$, gekürzt, heißt eine **"ultra"-beste Approximation** (kurz Ultra-Aproximation), an $0 < a \in /R$, wenn $|a \cdot v - u| > |a \cdot q - p| \; \forall \; 0 < v < q, u/v \neq p/q \; (u, v, p, q \in /N)$.

Schreibweise: $u(u/v, a) := |a \cdot v - u|$ "Ultra-Abstand".

Lemma: Jede Ultra-Approximation an a ist auch distanz-beste-Approximation an a.

Beweis: p/q sei Ultra-Approximation.
$|a \cdot v - u| > |a \cdot q - p| \; \forall \; u/v$.
$|a \cdot q - p| < |(a \cdot v)q - u/q| = 1/q \, |a \cdot v - u| = 1/v(a \cdot v - u) = |a - u/v|$.

Satz: Die reelle Zahl $Q < a \in /R$ habe die Kettenbruchentwicklung $[Q_0;Q_1,...]$. Dann sind die Näherungsbrüche $A_k = (-y_{k+1}/x_{k+1})$ für $k = 0$ Ultra-Approximation an a.

Beweis: $p_k = (-1)^{k+1} \cdot y_{k+1} = 0$; $q_k = (-1)^k \cdot x_{k+1} > 0$;
$A_k = p_k/q_k > 0$.

Satz: a sein $[Q_0;Q_1,...]$, unendlich oder abbrechend mit $Q_n = 2$, d.h. $a = [Q_0;Q_1,...,Q_n]$.
Dann gilt: $|a \cdot q_k - p_k| > |a \cdot q_{k+1} - p_{k+1}|$ für $k = 0$.

Beweis: $a = [Q_0;Q_1,...,Q_k,Q_{k+1},...]$ mit $[Q_{k+1},...] := Q'_{k+1} \in /R$
daraus folgt $a = [Q_0;Q_1,...,Q_k,Q'_{k+1}]$ mit $Q'_{k+1} \in /R$.

[Zur vorangehenden Stunde (15.01.04),
zur nächsten Stunde (20.01.04),
zur Protokollübersicht]

Satz 1 Es sei $\alpha \in \mathbb{R}$ und $\alpha = [Q_0; Q_1, \ldots]$ eine unendliche oder abbrechende Kettenbruchentwicklung mit $Q_n \geq 2$. Dann ist

$$|\alpha q_k - p_k| > |\alpha q_{k+1} - p_{k+1}|$$

für alle $k \in \mathbb{N}_0$.
Beweis. Nach unserer Notation ist

$$\alpha = [Q_0; Q_1, Q_2, \ldots, Q_k, Q_{k+1}, \ldots]$$

und

$$A_{k+1} = [Q_0; Q_1, Q_2, \ldots, Q_k, Q_{k+1}].$$

Um α und A_{k+1} vergleichen zu können, definieren wir daher $Q'_{k+1} \in \mathbb{R}$ durch

$$Q'_{k+1} := [Q_{k+1}, Q_{k+2}, \ldots]$$

und erhalten

$$\alpha = [Q_0; Q_1, Q_2, \ldots, Q_k, Q'_{k+1}] =: A'_{k+1} = -\frac{y'_{k+2}}{x'_{k+2}}.$$

Nach §7, Satz 3 (Beweis) ist die Iterationsformel für das Paar (x_{i+2}, y_{i+2}) gegeben durch

$$\begin{bmatrix} x_{i+1} & y_{i+1} \\ x_{i+2} & y_{i+2} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -Q_{i+1} \end{bmatrix} \cdot \begin{bmatrix} x_i & y_i \\ x_{i+1} & y_{i+1} \end{bmatrix}.$$

Wenden wir diese Formel auf (x'_{i+2}, y'_{i+2}) an, so erhalten wir

$$(*) \quad \begin{bmatrix} x_{k+1} & y_{k+1} \\ x'_{k+2} & y'_{k+2} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -Q'_{k+1} \end{bmatrix} \cdot \begin{bmatrix} x_k & y_k \\ x_{k+1} & y_{k+1} \end{bmatrix}.$$

Dabei ist die Matrix

$$M_k := \begin{bmatrix} x_k & y_k \\ x_{k+1} & y_{k+1} \end{bmatrix} \in GL(2, \mathbb{Z})$$

mit $\det M_k = (-1)^{k+1}$ und

$$M_k^{-1} = (-1)^{k+1} \begin{bmatrix} y_{k+1} & -y_k \\ -x_{k+1} & x_k \end{bmatrix}.$$

Multiplizieren wir nun (*) von rechts mit M_k^{-1}, so erhalten wir

$$\begin{bmatrix} x_{k+1} & y_{k+1} \\ x'_{k+2} & y'_{k+2} \end{bmatrix} \cdot \begin{bmatrix} y_{k+1} & -y_k \\ -x_{k+1} & x_k \end{bmatrix} = (-1)^{k+1} \begin{bmatrix} 0 & 1 \\ 1 & -Q'_{k+1} \end{bmatrix}.$$

Als Eintrag in der 2. Zeile und 2. Spalte bekommen wir

$$-x'_{k+2} y_k + y'_{k+2} x_k = -(-1)^{k+1} Q'_{k+1}$$

bzw.

$$x'_{k+2} y_k - y'_{k+2} x_k = (-1)^{k+1} Q'_{k+1},$$

der Eintrag in der 2. Zeile und 1. Spalte ist gegeben durch

$$x'_{k+2} y_{k+1} - y'_{k+2} x_{k+1} = (-1)^{k+1} \cdot 1 = (-1)^{k+1}.$$

Division dieser beiden Gleichungen liefert

$$\begin{aligned} Q'_{k+1} &= \frac{x'_{k+2}y_k - y'_{k+2}x_k}{x'_{k+2}y_{k+1} - y'_{k+2}x_{k+1}} \\ &= \frac{y_k - \frac{y'_{k+2}}{x'_{k+2}}x_k}{y_{k+1} - \frac{y'_{k+2}}{x'_{k+2}}x_{k+1}} \\ &= \frac{y_k - A'_{k+1}x_k}{y_{k+1} - A'_{k+1}x_{k+1}} \\ &= \frac{y_k - \alpha x_k}{y_{k+1} - \alpha x_{k+1}} \\ &= -\frac{\alpha q_{k-1} - p_{k-1}}{\alpha q_k - p_k}. \end{aligned}$$

Mit anderen Worten:

$$|\alpha q_{k-1} - p_{k-1}| = Q'_{k+1}|\alpha q_k - p_k| > |\alpha q_k - p_k|,$$

denn

$$Q'_{k+1} = Q_{k+1} + \frac{1}{Q_{k+2} + \ldots} > 1$$

nach Voraussetzung. ||

Satz 2 Die $A_k = \frac{p_k}{q_k}$ sind für $k \geq 1$ Ultra-Approximationen an α.
Beweis. Es sei $\frac{u}{v} \in \mathbb{Q}$ mit $\frac{u}{v} > 0$, $0 < v \leq q_k$ und $\frac{u}{v} \neq \frac{p_k}{q_k}$ gegeben. Um nun zeigen zu können, dass $|\alpha q_k - p_k| < |\alpha v - u|$ ist, benötigen wir eine Gleichung zwischen (p_k, q_k) einerseits und (u, v) andererseits. Per Definition ist

$$p_k = (-1)^{k+1}y_{k+1} \quad \text{und} \quad q_k = (-1)^k x_k.$$

Wir betrachten nun die invertierbare Matrix

$$N_k := \begin{bmatrix} -x_k & y_k \\ x_{k+1} & -y_{k+1} \end{bmatrix} = (-1)^k \begin{bmatrix} q_{k-1} & p_{k-1} \\ q_k & p_k \end{bmatrix}$$

und das $\mathbb{Z}$-lineare Gleichungssystem

$$(\#) \quad \begin{bmatrix} s & r \end{bmatrix} \cdot \begin{bmatrix} q_{k-1} & p_{k-1} \\ q_k & p_k \end{bmatrix} = \begin{bmatrix} u & v \end{bmatrix}$$

mit Lösung $\begin{bmatrix} s & r \end{bmatrix}$. Mit (#) erhalten wir

$$\alpha v - u = \alpha(sq_{k-1} + rq_k) - (sp_{k-1} + rp_k) = s(\alpha q_{k-1} - p_{k-1}) + r(\alpha q_k - p_k).$$

Aus dem Beweis des vorhergehenden Satzes haben wir außerdem die Beziehung $\alpha q_{k-1} - p_{k-1} = -Q'_{k+1}(\alpha q_k - p_k)$ und erhalten damit

$$\alpha v - u = (-sQ'_{k+1} + r)(\alpha q_k - p_k) = (r - sQ'_{k+1})(\alpha q_k - p_k).$$

Weiter gilt:
(1) Es ist $s \neq 0$, denn wäre $s = 0$, so folgte $v = rq_k$ und $u = rp_k$ und damit

$$\frac{u}{v} = \frac{p_k}{q_k}$$

im Widerspruch zur Voraussetzung.
(2) Es ist $Q'_{k+1} > 1$ (siehe oben).
(3) Ist $r \neq 0$, so haben r und s entgegengesetzte Vorzeichen:
Angenommen, r und s wären beide negativ. Dann folgte

$$v = sq_{k-1} + rq_k < 0$$

im Widerspruch zu $v > 0$.
Angenommen, r und s wären beide positiv, so wäre

$$v = sq_{k-1} + rq_k > q_k,$$

da $r, s \in \mathbb{Z}$ sind und damit $r, s \geq 1$ gelten würde. Dies ist aber ein Widerspruch zu $v \leq q_k$.
Damit ist für alle $r \in \mathbb{Z}$

$$| - sQ'_{k+1} + r| = |s|Q'_{k+1} + |r|$$

und wir erhalten insgesamt

$$|\alpha v - u| = (|s|Q'_{k+1} + |r|)|\alpha q_k - p_k| > |\alpha q_k - p_k|. \qquad ||$$

Als kleine Anwendung wollen wir die näherungsweise Berechnung von $x = \sqrt{n^2+1}$ für ein $n \in \mathbb{N}$ betrachten (zum Beispiel $\sqrt{2}, \sqrt{5}, \sqrt{50}, \ldots$: In der Schule kann man dies mittels verschiedener Verfahren machen:
a) Intervallschachtelung / probieren.
b) Heron-Verfahren.
c) Man betrachte den Ansatz $n^2 + 1 = (a + b)^2$ für $a \gg b$, zum Beispiel $a = n$. Dann ist

$$n^2 + 1 = (n + b)^2 = n^2 + 2nb + b^2$$

bzw. (da $n \gg b \gg b^2$)

$$1 \approx 2nb$$

und damit

$$b \approx \frac{1}{2n}.$$

Wir erhalten

$$x = \sqrt{n^2+1} \approx n + \frac{1}{2n}.$$

d) Ein andere Ansatz wäre etwa die Beziehung $x = \sqrt{n^2+1}$ umzuformulieren in

$$(x + n)(x - n) = 1.$$

Dies ergibt

$$x = n - \frac{1}{n+x} = n - \frac{1}{n + n - \frac{1}{n+x}} = n - \frac{1}{2n - \frac{1}{n+x}} = \ldots,$$

also eine Kettenbruchentwicklung und damit die beste Approximation für $x = \sqrt{n^2+1}$.
(Für die Schule betrachte man etwa auch: Kießwetter, *In über 3000 Jahren angewachsen [...]* aus *Der Mathematikunterricht (MU)*, HB: Z5577, Heft 3, Seite 23 - 33.)

Elementare Zahlentheorie WS 2003/04

Protokoll 22.01.2004 (AZ)

§ 9 B: Der Goldene Schnitt (EB)

Zur vorangehenden Stunde (20.01.04),
zur nächsten Stunde (23.01.04),
zur Protokollübersicht.
[Das Protokoll ist noch nicht redigiert.]

Frage: Was ist der Goldene Schnitt?

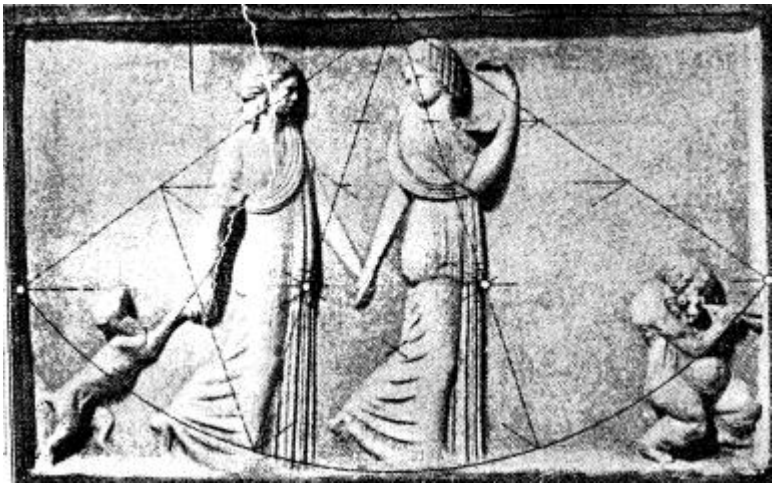
Definition: $\overline{AB}$ sei eine Strecke. Ein Punkt S auf der Strecke $\overline{AB}$ teilt $\overline{AB}$ im Goldenen Schnitt, falls sich die größere Teilstrecke zur kleineren so verhält wie die Gesamtstrecke zur größeren Teilstrecke.

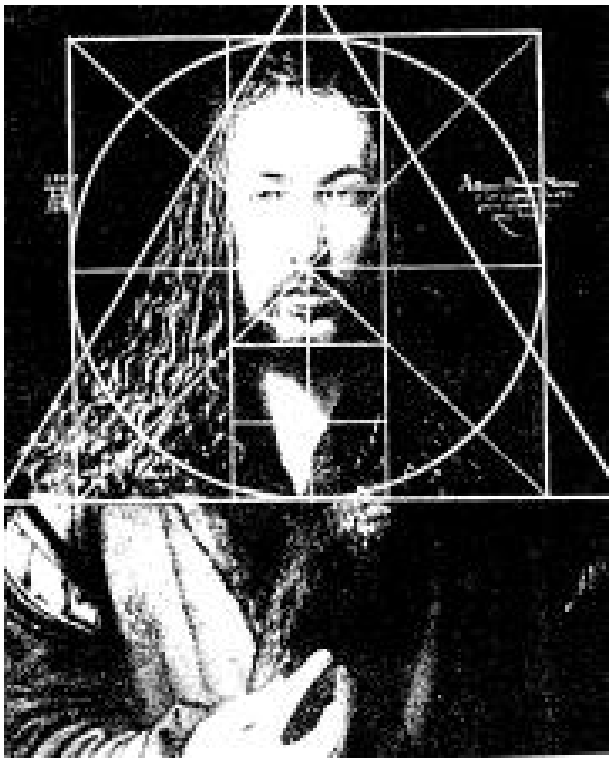
Dabei gibt es immer zwei Möglichkeiten für den Schnitt, nämlich eine von links und eine von rechts.

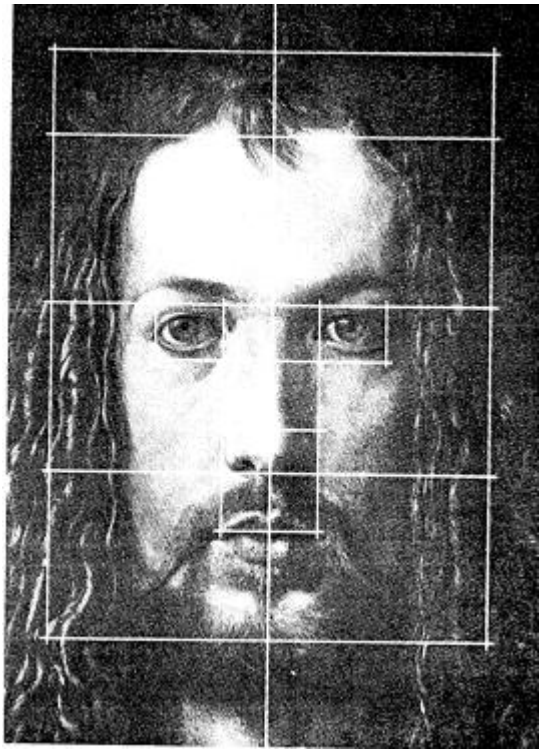
Sei $\overline{AB}$ eine Strecke der Länge a. Ein Punkt S auf $\overline{AB}$ teilt die Strecke im Goldenen Schnitt, falls $\frac{M}{m} = \frac{a}{M}$, das heißt genau dann, wenn $M^2 = am$.

Behauptung: Genau dann teilt ein Punkt S die Strecke $\overline{AB}$ im Goldenen Schnitt, wenn $\frac{M}{m} = \frac{1+\sqrt{5}}{2} \approx 1{,}618$ ist.

Beispiele aus der Kunst zeigen, dass der Goldene Schnitt in Kunst und Architektur sehr bedeutend ist. Man will nicht alles zentrieren, um Bilder und Bauwerke interessanter zu machen. Außerdem wird das Auge gerade von Dingen angezogen, die nicht mittig sind.







Beweis der Behauptung:

| $\overline{AB}$ | = a , also a = M + m

zu zeigen:

$$\frac{M}{m} = \frac{1+\sqrt{5}}{2} \approx 1{,}618$$

dazu: $M^2 = am$

$M^2 = (M + m)m = Mm + m^2$

$$\frac{M^2}{m^2} = \frac{M}{m} + 1,$$
$$\frac{M^2}{m^2} - \frac{M}{m} - 1 = 0,$$
$$\frac{M}{m} = \frac{1+\sqrt{5}}{2}.$$

Da die negative Lösung nicht möglich ist, ergibt sich $\frac{M}{m} = \frac{1+\sqrt{5}}{2} \approx 1{,}618$.

Ein alternativer Beweis ist:

$$\frac{M}{m} = \frac{a}{M} = \frac{M+m}{M} = 1 + \frac{m}{M} = 1 + \frac{1}{1+\frac{M}{m}} = \left[1, \bar{1}\right] = \frac{1+\sqrt{5}}{2}.$$

Wir bezeichnen nun

$$\frac{1+\sqrt{5}}{2} = \Phi.$$

Charakteristische Eigenschaften von Φ :

(1) $\Phi^2 = \Phi + 1$

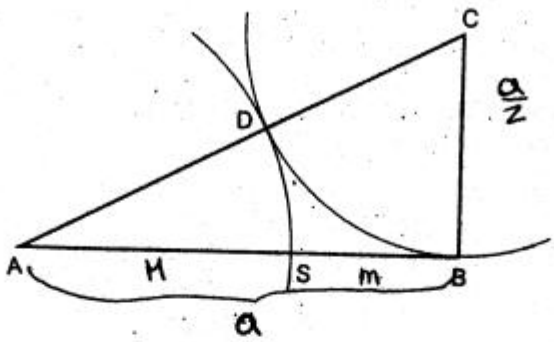
(2) $\frac{1}{\Phi} = \Phi - 1$

(3) $\Phi + \frac{1}{\Phi} = \sqrt{5}$

1. Konstruktion.

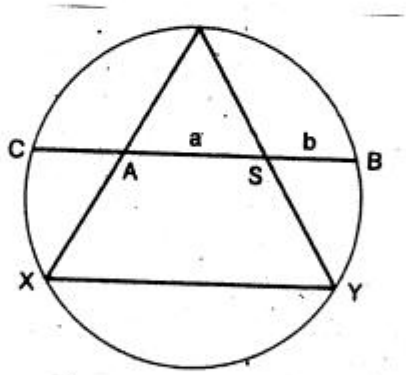
Sei $\overline{AB}$ eine Strecke der Länge a. Man errichte das Lot $\overline{BC}$ in B mit $|BC| = a/2$. Der Kreis um C mit Radius $|CB|$ trifft $\overline{AC}$ in einem Punkt D.

Der Kreis mit Radius $|AD|$ um A schneidet $\overline{AB}$ in S.



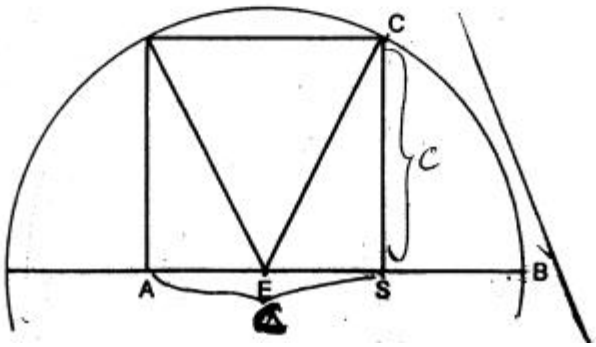
3. Konstruktion (George ODOM 1982).

Sei ΔXYZ ein gleichseitiges Dreieck mit Umkreis *K*. Seien A und S die Mittelpunkte der Seiten $\overline{XZ}$ und $\overline{YZ}$. Die Mittelparallele SA möge den Kreis *K* in den Punkten C und B treffen.



4. Konstruktion.

Sei $\overline{AS}$ eine Strecke. Man errichte in S das Lot $\overline{SC}$ mit $|SC| = |AS|$. Der Kreis um den Mittelpunkt E von $\overline{AS}$ mit dem Radius $|EC|$ trifft die Gerade AS (auf der Seite von S) in einem Punkt B.



Beweis zur Konstruktion1:

Zu zeigen:

$$\frac{|AB|}{|AS|} = \Phi$$

Dazu :

$$|AD| = (\sqrt{5}-1)\frac{a}{2} = \frac{a}{\Phi} = |AS| = M$$

$$|AC| = \sqrt{\frac{a^2}{4}+a^2} = \sqrt{5}\frac{a}{2}$$

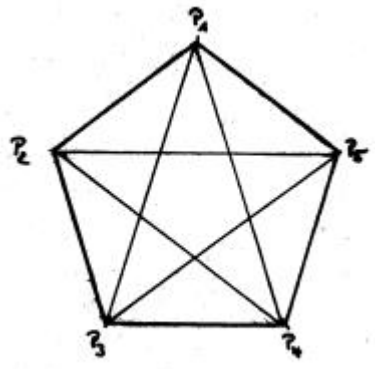
$$\frac{|AB|}{|AS|} = \frac{a}{\frac{a}{\Phi}} = \Phi.$$

Beweis zur Konstruktion 4:

$$\frac{|AB|}{|AS|} = \Phi$$

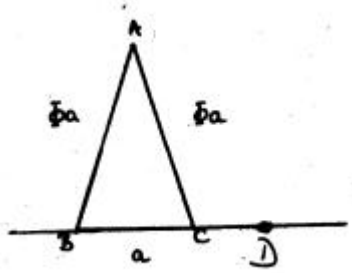
$$dazu: \frac{|AB|}{|AS|} = \frac{\frac{c}{2}+\sqrt{\frac{c^2}{4}+c^2}}{c} = \frac{\frac{c}{2}+\sqrt{\frac{5}{4}c^2}}{c} = \frac{\frac{c}{2}+\frac{\sqrt{5}}{2}c}{c} = \frac{1}{2}+\frac{\sqrt{5}}{2} = \Phi.$$

Das reguläre Fünfeck:



Das Verhältnis einer Diagonalen zu einer Seite ist ein Goldener Schnitt.

Das Goldene Dreieck:



Das Verhältnis der Schenkel zur Basis ist gleich Φ .

Frage: Wie kann man aus einer Strecke ein Goldenes Dreieck konstruieren?

Man geht von der Basis als vorgegebene Strecke aus. Dann konstruiert man einen weiteren Punkt Φ a wie in Konstruktion 4. Dann zieht man um die Eckpunkte der Basis einen Kreis mit Radius Φ a.

Das Goldene Rechteck:

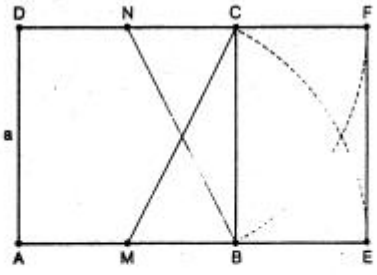
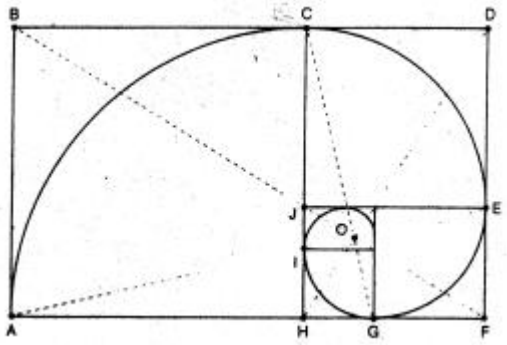


Bild 3.1

Konstruktion: Sei ABCD ein Quadrat. Der Kreis um den Mittelpunkt M von $\overline{AB}$ mit Radius |MC| schneidet die Verlängerung der Strecke $\overline{AB}$ in einem Punkt E. Entsprechend schneidet der Kreis um den Mittelpunkt N von $\overline{DC}$ die Verlängerung von $\overline{DC}$ (auf der Seite von E) in einem Punkt F.

Die Goldene Spirale:

Die Goldene Spirale entsteht, indem man ein Goldenes Rechteck in ein Quadrat und ein neues Goldenes Rechteck aufteilt, das man dann wieder aufteilt und so weiter.



Beweis, dass das kleinere Dreieck wieder Golden ist:

$$\frac{a}{\Phi a - a} = \frac{a}{(\Phi - 1)a} = \frac{a}{\frac{a}{\Phi}} = \Phi$$

Zur vorangehenden Stunde (20.01.04),
zur nächsten Stunde (23.01.04),
zur Protokollübersicht.

Elementare Zahlentheorie WS 2003/04

Stundenprotokoll zum 23.01.2004

Verhältniszahlen des Goldenen Schnittes

1 : 0,6	21 : 13,0	41 : 25,3	61 : 37,7	81 : 50,1
2 : 1,2	22 : 13,6	42 : 26,0	62 : 38,3	82 : 50,7
3 : 1,9	23 : 14,2	43 : 26,6	63 : 38,9	83 : 51,3
4 : 2,5	24 : 14,8	44 : 27,2	64 : 39,6	84 : 51,9
5 : 3,1	25 : 15,5	45 : 27,8	65 : 40,2	85 : 52,5
6 : 3,7	26 : 16,1	46 : 28,4	66 : 40,8	86 : 53,2
7 : 4,3	27 : 16,7	47 : 29,0	67 : 41,4	87 : 53,8
8 : 4,9	28 : 17,3	48 : 29,7	68 : 42,0	88 : 54,4
9 : 5,6	29 : 17,9	49 : 30,3	69 : 42,6	89 : 55,0
10 : 6,2	30 : 18,5	50 : 30,9	70 : 43,3	90 : 55,6
11 : 6,8	31 : 19,2	51 : 31,5	71 : 43,9	91 : 56,2
12 : 7,4	32 : 19,8	52 : 32,1	72 : 44,5	92 : 56,9
13 : 8,0	33 : 20,4	53 : 32,8	73 : 45,1	93 : 57,5
14 : 8,7	34 : 21,0	54 : 33,4	74 : 45,7	94 : 58,1
15 : 9,3	35 : 21,6	55 : 34,0	75 : 46,4	95 : 58,7
16 : 9,9	36 : 22,2	56 : 34,6	76 : 47,0	96 : 59,3
17 : 10,5	37 : 22,9	57 : 35,2	77 : 47,6	97 : 59,9
18 : 11,1	38 : 23,5	58 : 35,8	78 : 48,2	98 : 60,6
19 : 11,7	39 : 24,1	59 : 36,5	79 : 48,8	99 : 61,2
20 : 12,4	40 : 24,7	60 : 37,1	80 : 49,4	100 : 61,8

Erklärung der Zahlen anhand eines Beispiels:
13 : 8,0 → Länge von 13 cm; nach 8 cm setzt man den goldenen Schnitt.

13, 21, 34, 55, 89 haben ein gerades Verhältnis. Sie sind *Fibonacci-Zahlen*!

Fibonacci-Folge:
0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, …

Definition: $f_{n+2} = f_{n+1} + f_n \qquad f_0 = 0, f_1 = 1$

Formel von Binet: $$f_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$$

Fibonacci (1180 – 1250):
Er hieß ursprünglich Leonardo von Pisa und war der Sohn eines Kaufmannes von Bonacci (filius de Bonacci → Fibonacci). Sein Vater betrieb viel Handel in arabischen Ländern, zudem hatte

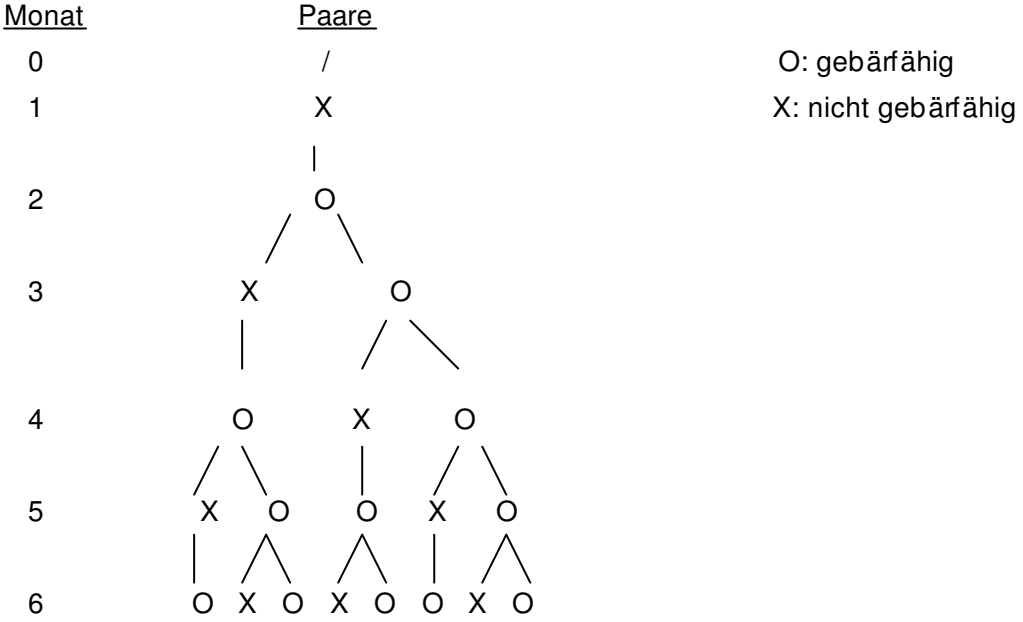
Fibonacci arabische Lehrer, so dass er mit den Rechenmethoden und der Mathematik der Araber bekannt wurde und diese in Europa einführte.

1. Beispiel: Kaninchenaufgabe

(i) Jedes Paar ist ab dem 2. Monat gebärfähig.

(ii) Jedes Paar bringt von da an ein neues Paar zur Welt.

(8) Alle Kaninchen leben ewig.



Die Fibonacci-Folge ist die Lösung dieser Aufgabe!

2. Beispiel:

Ein Briefträger muss jeden Tag 40 Stufen hinaufgehen. Die erste Stufe betritt er immer. Ab der zweiten Stufe hat er die Wahl, eine oder zwei Stufen auf einmal zu nehmen. Wie viele Möglichkeiten gibt es, zur vierzigsten Stufe zu gelangen?
(Die Lösung ist auch wieder die Fibonacci-Folge.)

F und Fibonacci

$u_1 = \phi^1, u_2 = \phi^2, ..., u_n = \phi^n$

Zu zeigen: (i) u verhält sich wie die Fibonacci-Folge: $u_{n+2} = u_{n+1} + u_n$

(ii) $v_n = \left(-\frac{1}{\phi}\right)^n$ $\qquad v_{n+2} = v_{n+1} + v_n$ **Lucas-Folge**

Beweis: (i) $\phi^n + \phi^{n+1} = \phi^n (1+\phi) = \phi^{n+2}$

Lucas-Folge

Für jede Lucas-Folge $(a_1,...,a_k)$ und für alle k = 2 gilt:

$$a_{k+1} = f_k \cdot a_2 + f_{k-1} \cdot a_1 .$$

Daraus folgt

$$\phi^n = f_n \cdot \phi + f_{n-1} ,$$

$$\left(-\frac{1}{\phi}\right)^n = f_{n-1} \cdot \frac{-f_n}{\phi} .$$

-

-

Beweis zur Formel von Binet:

$$f_n = \frac{\phi^n - \left(-\frac{1}{\phi}\right)^n}{\sqrt{5}} \qquad f_n \approx \left\lfloor \frac{\phi^n}{\sqrt{5}} \right\rfloor$$

$$\phi^n - \left(-\frac{1}{\phi}\right) = f_n \cdot \phi + f_{n-1} - f_{n-1} + \frac{f_n}{\phi} = ... = f_n \cdot \sqrt{5}.$$

$$\phi = \frac{M}{m} \approx \frac{f_{n+1}}{f_n}$$

Besprechung der Aufgabe 7

$$\frac{1+\sqrt{5}}{2} = 2 + \frac{\sqrt{5}-1}{2} = 1 + \frac{1}{\frac{2}{\sqrt{5}-1}} = 1 + \frac{1}{\frac{2(\sqrt{5}-1)}{4}} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{\sqrt{5}-1}{2}}}$$

$$\phi = [1;\overline{1}]$$

Mit dem PC:

- Spalten für Q_i definieren,
- Q_{i+1} wegfallen lassen,

- rekursiv berechnen.

k	x	y
-1	1	0
0	0	1
1	1 – 1·0 = 1	0 - 1·1 = -1
2	0 – 1 = -1	1 + 1 = 2
3	1 + 1 = 2	-3
4	-1 – 2 = -3	5
5	5	-8
6	-8	

$$a_{i-1} - Q_i a_i = a_{i+1}$$

$$A_k = \frac{-y_{k+1}}{x_{k+1}}$$

$$\sqrt{2} = [1,\overline{2}] \qquad \Leftrightarrow \quad \phi = [1;\overline{1}] \quad ?$$
$$\sqrt{5} = [2,\overline{4}]$$

$$x_k \geq f_k$$

$$\left|\alpha - A_k\right| \leq \frac{1}{x_k^2}$$

$$\begin{bmatrix} f_n \\ f_{n+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} f_{n-1} \\ f_n \end{bmatrix}$$

$$\begin{bmatrix} f_1 \\ f_2 \end{bmatrix} = A^1 \cdot \begin{bmatrix} f_0 \\ f_1 \end{bmatrix} = A \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} f_i \\ f_{i+1} \end{bmatrix} = A^i \cdot \begin{bmatrix} f_0 \\ f_1 \end{bmatrix}$$

$$T \cdot A \cdot T^{-1} = D = \begin{bmatrix} \phi & \\ & -\frac{1}{\phi} \end{bmatrix} \qquad T \cdot A^n \cdot T^{-1} = D^n = \begin{bmatrix} \phi^n & \\ & \left(-\frac{1}{\phi}\right)^n \end{bmatrix}$$

$$c_A(x) = \det\begin{bmatrix} -x & 1 \\ 1 & 1-x \end{bmatrix} = -x(1-x) = x^2 - x - 1 : \phi, -\frac{1}{\phi}$$

$$A^n = T^{-1} \cdot \begin{bmatrix} & \\ & \end{bmatrix} \cdot T$$

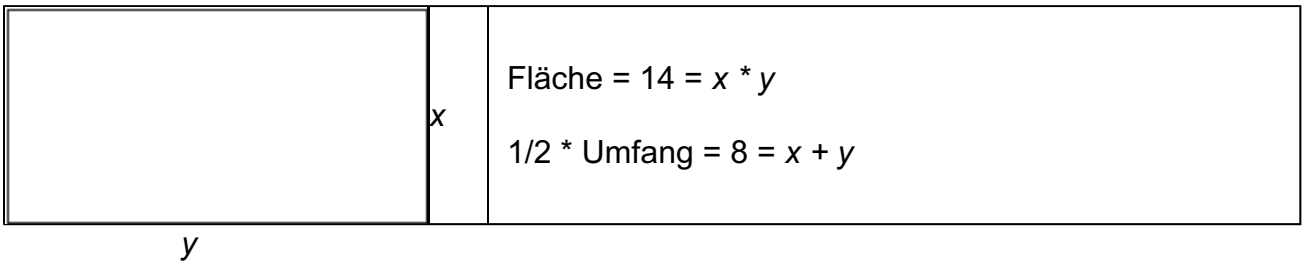
[Zur vorangehenden Stunde (23.01.04),
zur nächsten Stunde (29.01.04),
zur Protokollübersicht]

Quadratische Gleichungen und iterative Lösungen

Vorlesung "Elementare Zahlentheorie" vom 27.01.2004 (NB)

Inhalt: § 9 D: Vergleich mit Heron-Verfahren (SM + AZ)

Betrachte folgendes Rechteck:



Gesucht ist nun eine Lösung für (*x, y*), wobei iterativ vorgegangen werden soll (d.h. keine Benutzung der p/q-Formel).

Folgende Idee: Man gibt sich einen Wert in einer Formel beliebig vor, damit berechnet man den zweiten Wert aus. Diesen setzt man in die erst Formel ein und erhält einen neuen Wert für die erste Variable. Diese setzt man nun wieder in die andere Formel ein usw.:

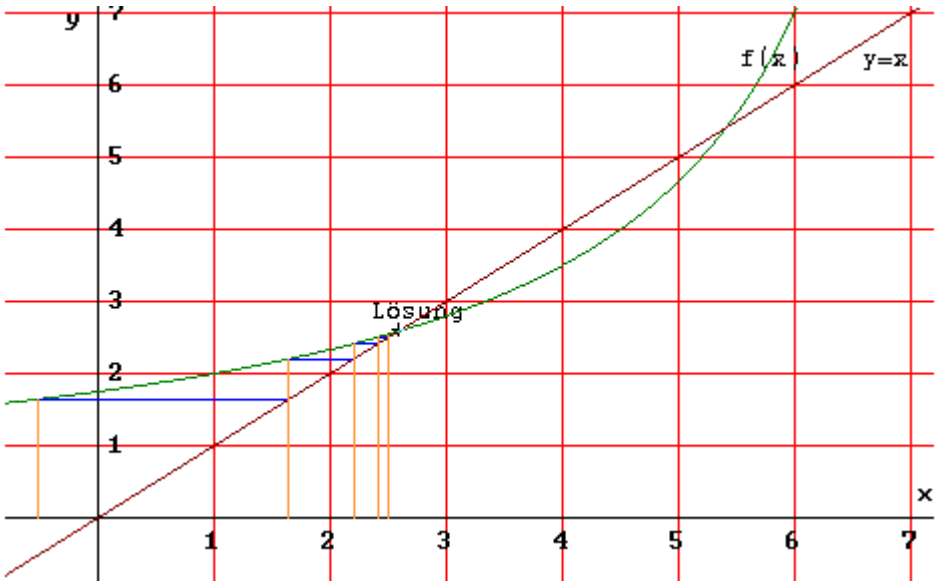
Gebe in der Umfangsformel $x_1 = 3$ vor:

A) [Umfangsformel] $y_1 = 8 - x_1 = 8 - 3 = 5$
B) [Flächenformel] $x_2 = 14 / y_1 = 14 / 5 = 2,8$
A') [Umfangsformel] $y_2 = 8 - x_2 = 8 - 2,8 = 5,2$
B') [Flächenformel] $x_3 = 14 / y_2 = 14 / 5,2 \approx 2,69$
A'') [Umfangsformel] $y_3 = 8 - x_2 = 8 - 2,69 = 5,31$
.
.
.
B^{n-1}) [Flächenformel] $y_n = 8 - x_n = 8 - 2,59 = 5,41$
A^n) [Umfangsformel] $x_{n+1} = 14 / y_n = 14 / 5,41 \approx 2,59$

Betrachten wir also noch einmal die Formeln:

$$x = \frac{14}{8-x} := f(x) \quad , \quad x = 8 - \frac{14}{x}$$

und den Graphen von *f(x)*:



Hier sieht man das Verfahren graphisch verdeutlicht. Die orangen Striche markieren dabei gerade die jeweils neuen *x* -Werte.

Führen wir zuletzt die Sache auf eine verallgemeinerte Kettenbruchentwicklung zurück:

$$x = \frac{14}{8-x} = \cfrac{14}{8-\cfrac{14}{8-\cfrac{14}{8-\ddots}}}$$

$$8-\ddots$$

$$\frac{14}{8-x_0}$$

Wenn man sich den Graphen genauer ansieht, sieht man eine Symmetrie der beiden Lösungen (Punktspiegelung an (4,0)). Also verschieben wir die Funktion so, so dass (4,0) in den Ursprung kommt.

D.h. für
*-b = x * y*
a = y - x
*=> -b = x * (x +a)*
gilt:

allgemein	***bei uns***
*x * (x + a) = -b*	*14 = x * (8 - x)*
Setze z := x + a/ 2	Setze *z := x - 4*
*(z - a/2) * (z + a/2) = b*	*14 = (z + 4) * (4 - z)*

$z^2 - a^2/4 = -b$ => $z_{1,2} = \pm\sqrt{\frac{a^2}{4} - b} \Rightarrow x_{1,2} = -\frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b}$	$14 = 16 - z^2$ $z_{1,2} = \pm\sqrt{2} \Rightarrow x_{1,2} = 4 \pm \sqrt{2}$

Nun zum zweiten Teil der Vorlesung:

Berechnung von Wurzeln, speziell Lösung zu $x^2 = 2$

Das HERON-Verfahren

F: Wie kann man (Quadrat-)Wurzeln berechnen?

1) Geometrischer Zugang:

	x	*a* ist der Flächeninhalt des Rechtecks. Dann gilt: *x' = (x + y) / 2* und *y' = 2a / (x + y).*

y = a / x

2) Arithmetischer Zugang:

1. Abschätzung von $\sqrt{a}$. Man erhält *y*.
x < $\sqrt{a}$ < *y* oder *x* > $\sqrt{a}$ > *y.*

2. Bildung des arithmetischen Mittels:

*x' = 1/2 * (x + a/x)*

3. Abschätzung zwischen artihmetischem und geometrischem Mittel:

$$x' = \frac{1}{2}\left(x + \frac{a}{x}\right) > \sqrt{x \cdot \frac{a}{x}} = \sqrt{a}, \quad x > x' > \sqrt{a} > y' > y$$

4. Rekursionsfortschritt:

$x_0 > 0$ beliebig,

$x_{n+1} = 1/2\ (x_n + a/x_n)$

Satz: Für jeden Startwert $x_0 > 0$ konvergiert die Folge des Heronverfahrens gegen $\sqrt{a}$.

Beweis: [Z.z.: 1) $x_n > \sqrt{a}$ und 2) $x_n > x_{n+1}$]

Ad 1): Siehe 3. mit $x' := x_n$ und $x := x_{n-1}$.

Ad 2): Aus $x_n > \sqrt{a}$ folgt $a/x_n < \sqrt{a}$, also $x_n > a/x_n$, und x_{n+1} ist das arithmetische Mittel von x_n und y_n. Deswegen folgt: $x_n > x_{n+1}$. [Also ist die Folge streng monoton fallend und nach unten beschränkt, also konvergiert sie.] Bleibt nur noch zu zeigen, gegen welchen Wert sie konvergiert.

Beh.: $\sqrt{a}$ ist der Grenzwert.

Bew.: Es sei z der Grenzwert. Aus 1) folgt, dass $z \geq \sqrt{a} > 0$ ist. Also folgt aus $x_{n+1} = 1/2\ (x_n + a/x_n)$, $z = 1/2\ (z + a/z)$. Daraus folgt nach Auflösen nach z die Behauptung. ||

Frage nun: Wie groß ist der Fehler?

Nach n Schritten gilt:

$x_{n+1} - \sqrt{a} = 1/(2*x_n)\ (x_n - \sqrt{a})^2$. Man spricht in diesem Falle auch von quadratischer Konvergenz.

Satz: Die Anzahl der signifikanten Nachkommastellen verdoppelt sich bei jedem Schritt.

Beweis: Es sei $a > 1$. Es seien x_n und a/x_n in s Nachkommastellen genau, dann ist $x_n - \sqrt{a} < 10^{-s}$.
Also $x_{n+1} - \sqrt{a} = 1/(2 * x_n)\ (x_n - \sqrt{a})^2 < 1/2 * 10^{-2s}$.||

Zur vorangehenden Stunde (23.01.04),
zur nächsten Stunde (29.01.04),
zur Protokollübersicht.

Stundenprotokoll vom 30.01.2004

§ 9. F Das Planetarium von Christiaan Huygens

J. Kepler 1571 – 1630

René Descartes 1496 – 1650

Christiaan Huygens 1629 – 1695

Louis XIV 1638 – 1715

In einem Jahr dreht sich die Erde um die Sonne um 359°45’40’’31’’’ := a (?).

In einem Jahr dreht sich der Saturn um die Sonne um 12°13’35’’18’’’ := b.

Oeuvers S. 626

$$\frac{a}{b} = \frac{77708431}{2640858} = \frac{y}{x}$$

$$\frac{a}{b} = (29;2,2,1,5,1,4,...) \approx \frac{206}{7}$$

Dezimaldarstellung von $\alpha \in R$

$a_0 := \alpha$

$a_0 = \lfloor a_0 \rfloor + a_1 \quad , 0 \le a_1 < 1 \quad D_0 = \lfloor a_0 \rfloor$

$10a_1 = \lfloor 10a_1 \rfloor + a_2 \quad , 0 \le a_2 < 1 \quad D_1 = \lfloor 10a_1 \rfloor$

$10a_2 = \lfloor 10a_2 \rfloor + a_3 \quad , 0 \le a_3 < 1 \quad D_2 = \lfloor 10a_2 \rfloor$

Dezimaldarstellung $\alpha = D_0, D_1 D_2 ...$

$f(x) = 10x$

$\boxed{f(a_1) = \lfloor f(a_1) \rfloor + a_2}$

Kettenbruchdarstellung von $\alpha \in R$

$a_0 := \alpha$

$a_0 = \lfloor a_0 \rfloor + a_1 \quad , 0 \le a_1 < 1 \; ; Q_0 = a_0$

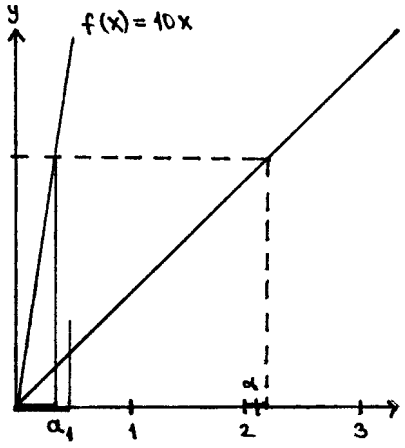
$(= \lfloor a_0 \rfloor + \frac{1}{1/a_1})$

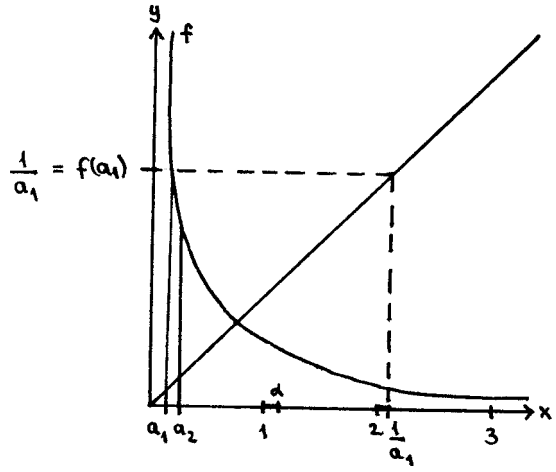
$\frac{1}{a_1} = \left\lfloor 1/a_1 \right\rfloor + a_2 \quad , 0 \le a_2 < 1 \; ; Q_1 = \left\lfloor 1/a_1 \right\rfloor$

$\frac{1}{a_2} = \left\lfloor 1/a_2 \right\rfloor + a_3$

$\alpha = (Q_0, Q_1 ...)$

$f(x) = \frac{1}{x}$





§ 10. Approximationsordnung

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k^2}$$ für konvergente $\frac{p_k}{q_k}$ an α.

Definition. $\alpha \in R$ heißt approximierbar von der Ordnung $n \in R$, wenn $\delta \in N$ existiert mit

$$\left|\alpha - \frac{a}{b}\right| < \frac{\delta}{b^n}$$ für unendlich viele $\frac{a}{b}(gekürzt) \in Q$, $b > 0$.

$$b^n \left|\alpha - \frac{a}{b}\right| < \delta$$

$= u_n(\frac{a}{b}, \alpha)$ „Ultra-Abstand der Ordnung n“.

Satz 1. Rationale Zahlen sind approximierbar von der Ordnung 1, aber nicht von der Ordnung $1+\varepsilon$ für $\varepsilon > 0$.

Beweis. $\alpha = \frac{r}{s} gegeben \in Q$.

(i) Betrachte $\frac{a}{b} := \frac{r}{s} + \frac{1}{v}$ für $v \in N$.

$$\left|\alpha - \frac{a}{b}\right| = \frac{1}{v} = \frac{s}{sv} \quad , \quad b|sv$$

$$< \frac{s+1}{sv} =: \frac{s}{sv} \leq \frac{\delta}{b} \quad . -$$

(ii) Gegeben [beliebiges] $\delta > 0$.

[Zu zeigen: Es existieren nur endlich viele $\frac{a}{b} \in Q$, gekürzt, mit

$\left|\alpha - \frac{a}{b}\right| < \frac{\delta}{b^{1+\varepsilon}}$.]

Für $\frac{a}{b} \neq \alpha = \frac{r}{s} : \left|\alpha - \frac{a}{b}\right| = \left|\frac{r}{s} - \frac{a}{b}\right| = \frac{|rb - as|}{sb} > \frac{1}{sb}$.

[Wir hoffen auf $\frac{1}{sb} \geq \frac{1}{b^{1+\varepsilon}}$ mit höchstens endlich vielen Ausnahmen.]

$\frac{1}{sb} < \frac{1}{b^{1+\varepsilon}}$ nur für $\frac{1}{s} < \frac{1}{b^{\varepsilon}}, b^{\varepsilon} < \delta \cdot s, b < (\delta \cdot s)^{\frac{1}{\varepsilon}}$: höchstens endlich viele $b \in N$.

Zu jedem b nur endlich viele $a \in N$ mit $\left|\alpha - \frac{a}{b}\right| < \frac{\delta}{b^{1+\varepsilon}}$; sonst $\left|\alpha - \frac{a}{b}\right| \geq \frac{\delta}{b^{1+\varepsilon}}$.||

Anwendung von der Idee aus Satz 1: $e \notin Q$.

Beweis: $e^x = 1 + x + \frac{1}{2!}x^2 + ...$

$$x = -1 : \frac{1}{e} = 1 - 1 + \frac{1}{2} - \frac{1}{3!} + ... + \frac{(-1)^n}{n!} + ...$$

Zitat: Ist $0 \leq a_0, a_1, \cdots$ in **R** monoton wachsend und unbeschränkt, so konvergiert

$$\sum_{k=0}^{\infty} \frac{(-1)^k}{a_k} = s \quad \text{mit} \quad 0 \leq \left| s - \sum^{n} \right| \leq \frac{1}{a_{n+1}} .$$

s_n

Setze $q_n = n!$

$$p_n = n!\sum_{k=0}^{n}\frac{(-1)^k}{k!} \in N \quad \Big\} \quad \frac{p_n}{q_n} \in Q \,.$$

$$0 < \left|\frac{1}{e} - \frac{p_n}{q_n}\right| = \left|\frac{1}{e} - s_n\right| < \frac{1}{(n+1)!} = \frac{1}{q_n(n+1)}$$

$$0 < \left|q_n \frac{1}{e} - p_n\right| < \frac{1}{n+1} \xrightarrow{n\to\infty} 0 \,.$$

Wäre $\frac{1}{e}$ rational, so $\alpha = \frac{1}{e} = \frac{a}{b}$: für beliebige $p, q \in Z$

$$q^{\alpha} - p = q\frac{a}{b} - p = \frac{1}{b}(qa - pb) \in Z\frac{1}{b}.$$ Widerspruch zu . |

Satz 2. $\alpha \in R$ sei irrational. Dann ist α approximierbar von der Ordnung *2*.

Klar nach Kettenbruch-Entwicklung: Konvergenten: s. o. (mit δ=1).

Satz 2'. (Hurwitz 1891). Ist $\alpha \in R/Q$, so gibt es unendlich viele Paare $(x, y) \in ZxN$ mit

$\left|\alpha - \frac{x}{y}\right| < \frac{1}{\sqrt{5}} \cdot \frac{1}{y^2}$ $\quad (\delta = \frac{1}{\sqrt{5}} < 1)$; falsch für kleinere δ.

[Hardy-Wright, S. 186, Satz 193-4]

Definition. $\alpha \in C$ heißt algebraisch [über Q] vom Grad n, wenn $0 \neq f(x) \in Q[X]$ vom Grad n existiert mit $f(\alpha) = 0$, aber keines von kleinerem Grad.

Satz. $\alpha \in R$ sei algebraisch vom Grad N ≥ 2.

a) In den Büchern steht nicht, dass dann α von der Ordnung N approximierbar sei.

b) (Lionville 1844). Es existiert $c > 0$ (zu α) mit

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^N}$$ für alle $(p, q) \in ZxN$.

c) α ist nicht von einer Ordnung ≥ $N+1$ approximierbar.

d) (K. F. Roth 1955). α algebraisch $\in R/Q$, $\varepsilon > 0$. Dann

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{q^{2+\varepsilon}}$$ für „fast alle“ $(p, q) \in ZxN$.

[Zur vorangehenden Stunde (30.01.04),
zur nächsten Stunde (05.02.04),
zur Protokollübersicht.]
[Das Protokoll ist noch nicht redigiert.]

Elementare Zahlentheorie

Stundenprotokoll vom 03.02.2004 (AW)

INHALT: Forts. von § 10: Approximationsordnung
Transzendente Zahlen (zum Beispiel e oder pi)
Approximationssatz

Fortsetzung von letzter Stunde:

α sei algebraisch von der Ordnung N. Dann ist α nicht approximierbar von einer Ordnung größer oder gleich N + 1.

Satz:

Wenn ein δ existiert mit $|\alpha - a/b|$ kleiner als δ/b^N für unendlich viele a/b (gekürzt) Element aus **Q**, dann ist α approximierbar.

Satz:

Definiere $\zeta := 1/10^{1!} + 1/10^{2!} + 1/10^{3!} + \ldots\ldots + \ldots..$

Es gilt: ζ ist transzendent, d.h. nicht algebraisch von irgendeiner Ordnung.

Beweis:

Setze $\zeta_k = p(k) / q(k) = 1/10^{1!} + 1/10^{2!} + 1/10^{3!} + \ldots\ldots + 1/10^{k!}$

Es folgt: $|\zeta - \zeta_k| = 10^{-(k+1)!} (1 + 1/ 10^{(k+2)! - (k+1)!} + 1/ 10^{(k+3)! - (k+1)!} + \ldots)$

ist kleiner gleich $10^{-(k+1)!} (1 + 1/10^{k} + 1/10^{k*k} + ...)$
geometrische Reihe

ist kleiner gleich $2 * 10^{-(k+1)!}$

$= 2/q(k)^{k+1}$

ist kleiner gleich $2/q(k)^N$ für k +1 größer gleich N.

Also: ζ approximierbar von Ordnung N für alle N (ζ transzendent).

§11 Farey Folgen

0

1

F1	0/1												1/1
F2	0/1						½						1/1
F3	0/1				1/3		½		2/3				1/1
F4	0/1			1/4	1/3		½		2/3	3/4			1/1
F5	0/1		1/5	1/4	1/3	2/5	½	3/5	2/3	3/4	4/5		1/1
F6	0/1	1/6	1/5	1/4	1/3	2/5	½	3/5	2/3	3/4	4/5	5/6	1/1

-
-
-

Fragen:

(1) Wie schafft man es, neue Gliederungen einzuordnen?

(2) Wann ist a/b kleiner als c/d?

(3) Studiere &.

(4) Eigenschaften von $F_{k.}$

Planen (Vermutungen):

(1) Man addiert Zähler und Zähler sowie Nenner und Nenner. Man erhält einen dazwischen liegenden Bruch.

(2) Die neuen Brüche in F_{k+1} sind von der Form a/b & c/d für konsekutive Brüche a/b, c/d (standen in der vorherigen Folge nebeneinander) in F_k.

(3) Folgerung: Die Determinante von konsekutiven Paaren in F_k ist -1.

(4) Ein Intervall in M_k (Medianprozess) enthält nur Brüche mit größeren Nennern als die Intervallenden als Nenner haben.

Schreiben (Beweise):

(1)

	a/b	ist kleiner als	c/d		
äqui.	ad	ist kleiner als	cb		
daraus folgt	ab + ad	ist kleiner als	ab + bc		
äqui.	a (b + d)	ist kleiner als	b (a + c)		
daraus folgt	a/b	ist kleiner als	a + c/ (b + d)	=	a/b & c/d

[Zur vorangehenden Stunde (30.01.04),
zur nächsten Stunde (05.02.04),
zur Protokollübersicht.]

Vortragsthemen Elementare Zahlentheorie

1. **Neuner- und Elferprobe für Brüche?** **§ 2**
   Peter Hilton and Jean Pedersen, Casting out nines revisited, *Mathematics Magazine* 54:4 (1981), 195--201. MB: Z 167.

2. **Rationale Zahlen als Dezimalbrüche**. IS, NB + DB, TF. **§ 5**
   Niedersächsisches Kultusministerium (Hg.), *Neue Technologien und Allgemeinbildung: Mathematik; Anregungen für den Unterricht*, Hannover: Berenberg, 1990. ISBN 3-88990-010-0. S. 177--199: Kap. 2.9 Probieren, Entdecken, Forschen -- am Beispiel periodischer Dezimalbrüche.
   F. Padberg, *Didaktik der elementaren Zahlentheorie*, smd, Herder, ^{2}1991. ISBN 3-411-76392-2. MB: 15714. S. 114--135: VIII: Systembrüche.
   Weitere Literatur in meinem Verzeichnis Literatur zur Algebra unter **Elementare Zahlentheorie**/Dezimalbrüche.

3. **Prüfcodes**. AK, MH, MP. **§ 3**
   J. Gallian and S. Winters, Modular arithmetic in the market place, *Amer. Math. Monthly* 95:6 (1985), 548--551. MB: Z 42.
   Weitere Literatur in meinem Verzeichnis Literatur zur Algebra unter **Elementare Zahlentheorie**/Prüfcodes.

4. **Analyse des XEA (Erw. Eukl. Algor.)**. GC. **§ 7**
   S. 226--227: Exercises, Section 2, No. 2 (G. E. Collins) in:
   John D. Lipson, *Elements of Algebra and Algebraic Computing*, Reading, MA: Addison-Wesley, 1981. MB: 11267.

5. **Iteration mit kontrahierenden Funktionen**. SM, AZ. **§ 9**
   S. 98--102 sowie 110--111 in:
   Berthold Schuppar, *Elementare Numerische Mathematik - Eine problemorientierte Einführung für Lehrer und Studierende*, Braunschweig: Vieweg, 1999. ISBN 3-528-06984-8. HB: Bf9727.
   A. Fricke, Quadratische Gleichungen und ihre iterative Lösung, *Praxis der Mathematik* 26:1 (1984), 3--12. HB: Z1757-26; MB: Z 101.

6. **Farey-Approximation und Kettenbrüche**. AG. **§ 7, 9, 11**
   Ian Richards, Continued fractions without tears, *Mathematics Magazine* 54:4 (1981), 163--171. MB: Z 167.

7. **Fibonacci-Folge und Goldener Schnitt**. EB, CM. **§ 9**
   John Knott, http://www.mcs.surrey.ac.uk/Personal/R.Knott/Fibonacci/fib.htm (gesehen 27. Aug. 2003).

8. **Pythagoreische Tripel**. **§ 8**

   Literatur in meinem Verzeichnis Literatur zur Algebra unter **Elementare Zahlentheorie**/Pythagoreische Zahlentripel.

   - Gestalt und Zahl. AW, AE.
     Heinrich Winter, Gestalt und Zahl -- zur Anschauung im Mathematikunterricht, dargestellt am Beispiel der Pythagoreischen Zahlentripel, S. 254--269 in: C. Selter and G. Walther (Hrsg.), *Mathematik als design-science: Festschrift für Erich Christian Wittmann*, Ernst Klett Grundschulverlag, 1999. ISBN 3-12-200060-1. AC Inst. f. Erzwiss.: U 2594.
   - Entdecken und beweisen. US, MA.
     U. Schoenwaelder, Manuskript *Pythagoreische Tripel* (22.10.03).
   - Gruppenoperation. ST.
     J. E. Hofmann, Beispiele zur unbestimmten Analytik im Sinne der Alten, *Der Mathematikunterricht* 9:5 (1963), 5 - 37 [insbesondere 5 - 11]. HB: Z5577-9.

Aufgaben Elementare Zahlentheorie

Aufgabe 1

Abgabe Fr 24.10.03 in der Übungsstunde.

Wählen Sie aus meinem Literaturverzeichnis zur Elementaren Zahlentheorie unter *Figurierte Zahlen* eine Quelle aus, die Sie

- ausleihen bzw. besorgen,
- lesen, studieren,

und aus der die Sie einen

- *für Sie interessanten Punkt* auswählen und
- auf einer halben Seite darstellen.

Aufgabe 2 und Aufgabe 3

Abgabe Fr 31.10.03 in der Übungsstunde.

Aufgabe 2. Beschreiben Sie die 7-er- und die 17-er-Probe und führen Sie diese an je einem hinreichend großen Beispiel aus.
Aufgabe 3. Verallgemeinern Sie den "Chinesischen Restesatz" von zwei Moduln auf drei oder mehr Moduln. Berechnen Sie beispielsweise $a_{2.9.11}$ für $a_2 = 1$, $a_9 = 7$, $a_{11} = 6$.

Aufgabe 4

Abgabe Fr 7.11.03 in der Übungsstunde.

Aufgabe 4 (Untergruppen zyklischer Gruppen).
a) Jede zyklische Gruppe ist isomorph zu einer Faktorgruppe der (additiven) Gruppe $\mathbf{Z}$ aller ganzen Zahlen.
b) Die Untergruppen von $\mathbf{Z}$ haben die Form

$$n\mathbf{Z} = \{nk \mid k \text{ in } \mathbf{Z}\}$$

für ein n in $\mathbf{N}$ ohne $\{0\}$.
c) Die Untergruppen von $\mathbf{Z}/n\mathbf{Z}$ haben die Form $U/n\mathbf{Z}$ für eine Untergruppe $n\mathbf{Z} \leq U \leq \mathbf{Z}$, wobei $U = m\mathbf{Z}$ für einen Teiler m (in $\mathbf{N}$ ohne $\{0\}$) von n gilt.
d) Zu jedem Teiler k von n gibt es in $\mathbf{Z}/n\mathbf{Z}$ genau eine Untergruppe $U/n\mathbf{Z}$ der Ordnung k.

Aufgabe 5

Abgabe Do 20.11.03 vor der Vorlesung.

Aufgabe 5 (Neue Kernlehrpläne in Mathematik für die Sekundarstufe I).

1. Lesen Sie den Entwurf für einen Kernlehrplan Mathematik/Sekundarstufe I NRW unter http://www.learn-line.nrw.de/angebote/kernlehrplaene/, Mathematik/Gymnasium anklicken.
2. Wie haben Sie (unmittelbar) auf die Lektüre reagiert?
3. Beantworten Sie Frage 7 - 8 des dort beiliegenden Fragebogens auf einem Blatt Papier.
4. Weitere Stellungnahme?

Aufgabe 6

Abgabe Di 9.12.03 vor der Vorlesung.

Aufgabe 6 (Octalbrüche).
Entwickeln Sie eine Theorie der Octalbruch-Entwicklung rationaler Zahlen und geben Sie jeweils Beispiele. Stellen Sie dabei (schon geordnete) Fragestellungen voran.

Hinweise.
a) Beispielsereien können interaktiv mit Maple erstellt werden, indem derselbe Befehl mit "korrigierten Zahlenwerten" wiederholt angeklickt wird. Die folgenden Maple-Befehle können nützlich sein:
convert(*n*, octal); iquo(*n, m,* 'r'); isprime(*n*); nextprime(*n*);

b) *Mit welcher Zahl muss man 1/7 multiplizieren, um näherungsweise einenatürliche Zahl zu erhlaten, die ein Octaldarstellung hat, die bis auf Kommaverschiebung und gewünschte Stellenzahl die Octalbruch-Darstellung von 1/7 ist?*

Aufgabe 7 und Aufgabe 8

Abgabe Di 20.01.04 vor der Vorlesung.

Aufgabe 7 (Endliche und unendliche Kettenbrüche).

1. Bestimmen Sie (endliche) Kettenbruchentwicklungen $[a_0; a_1, .., a_k]$ für die Zahlen 17/11, 11/31, 30/43, indem Sie sukzessive $a_0, a_1, .., a_k$ als ganzzahligen Anteil des jeweiligen Rest-Bruches nehmen.
2. Bestimmen Sie analog (periodische) Kettenbruchentwicklungen für die Zahlen v2, v3, v5. (Benutzen Sie *keine* numerischen Näherungen. Beachten Sie vielmehr, dass quadratisch-irrationale Nenner durch Erweitern rational gemacht werden können.)
3. Zeigen Sie, dass [1; 1, 1, 1, ...] = 1/2 (1 + v5) gilt.

Aufgabe 8 (Konvergenten via Tabellenkalkulation).
Benutzen Sie ein Tabellenkalkulationssystem (etwa EXCEL), um über den XEA mit den in Aufgabe 7 ermittelten oder genannten Quotienten Q_i Folgen von Näherungsbrüche A_j (sog. Konvergenten) für die Quadratwurzeln in Aufgabe 7.2 und 7.3 zu erhalten.
[Nach Umwandlung in Dezimalzahlen kann man den jeweiligen Fehler als Dezimalzahl erhalten (notfalls mit Maple).]