Zahlentheorie

KPH Stams WS 11

1.Einführung

1.1. Brainstorming

- Was versteht man unter Zahlentheorie?

Zahlentheorie

Die Mathematik ist die Königin der Wissenschaften, und die Zahlentheorie ist die Königin der Mathematik.

C.F. Gauß

- Elementare Zahlentheorie
- Algebraische Zahlentheorie
- Analytische Zahlentheorie
- Approximation und Transzedenz
- Multiplikative Zahlentheorie
- Additive Zahlentheorie
- Probalistische Zahlentheorie
- Algorithmische Zahlentheorie

1.2.News

- **Eulers Erbe**
- Mathematiker feiern Entdeckung in der Zahlentheorie

  Die moderne Mathematik, so sollte man meinen, befasst sich längst nur noch mit Fragen, die unendlich weit entfernt von allem sind, was ein durchschnittlich gebildeter Mensch je verstehen kann. Es mag daher überraschen, dass in der Fachwelt zurzeit die Lösung eines Problems gefeiert wird, das so einfach klingt, als könnten Grundschüler damit befasst werden. Es geht um die Frage, auf wie viele Weisen man eine natürliche Zahl als Summe darstellen ...
-
  27.01.2011 Süddeutsche Zeitung | München, Bayern, Deutschland

- **Die Eine-Million-Dollar-Frage**
- Neues Interesse an der Goldbach'schen Vermutung
- Wahrscheinlich gibt es einfachere Wege, eine Million Dollar zu verdienen; andererseits sind die Chancen vermutlich auch nicht schlechter, als die berühmten sechs Richtigen im Lotto zu erwischen: Der britische Verlag *Faber and Faber* hat ein Preisgeld von einer Million Dollar für denjenigen ausgelobt, der die Richtigkeit der so genannten Goldbach'schen Vermutung bestätigt. Der Preis ist Teil einer Werbekampagne für einen Roman über dieses große Rätsel der Zahlentheorie.
- Der Name des preußischen Mathematikers Christian Goldbach ist heute nur noch ein Begriff, weil er 1742 in einem Brief an seinen Kollegen Leonhard Euler eine Vermutung aufstellte, die in ihrer modernen Formulierung lautet: Jede gerade Zahl, die größer als 2 ist, lässt sich als Summe von zwei Primzahlen ausdrücken.

News-Fermat

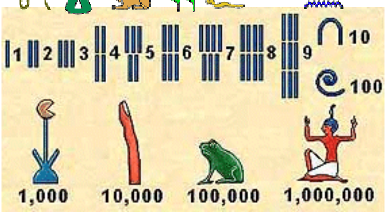
www.youtube.com/watch?v=7FnXgprKgSE

x^n+y^n=z^n für n>2 in ganzen Zahlen nicht lösbar

News

- **Quanten-Kryptografie geknackt ohne Spuren zu hinterlassen**
  30. August 2010 12:21 Standard
- Hacker können Quanten-Verschlüsselung mit Laser umgehen
- **Forschern ist es gelungen, zwei kommerzielle Systeme für Quanten-Verschlüsslung unbemerkt zu umgehen**
- Sicherheitsexperten von der norwegischen Universität in Trondheim soll es erstmals gelungen sein, zwei kommerzielle Systeme mit Quanten-Kryptografie zu knacken, ohne die Alarmglocken losschrillen zu lassen. Das berichtet Nature. Bislang galt es als unmöglich, derartig verschlüsselte Kommunikation auszuspionieren, ohne das System dabei merklich zu stören.

1.3.Die Arithmetik der Alten Ägypter



- Hieroglyphen
- Gruppierungssystem
- Additionssystem
- Dezimalsystem
- Zahl 0 ? („nichts“)

Multiplikation

- Beispiel: 14x27=?
- 1 27
- 2 54
- 4 108
- 8 216
- 16 432
- (2+4+8)x27 =54+108+216=378

Warum funktioniert das?

- Brainstorming

- Jede ganze Zahl lässt sich als Summe von Zweierpotenzen darstellen (Binärsystem)

Division

- Beispiel: 114:6
- 1 6
- 2 12
- 4 24
- 8 48
- 16 96
- Also: 114=6+12+96=6x(1+2+16)

Problem?

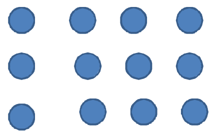
- Beispiel: 83:16=
- 1 16
- 2 32
- 4 64
- 8 128
- Also (1+4)*16=80 und 3 Rest!
- Brüche!

Brüche

- Beispiel: 83:16=
- 1 16
- 2 32
- 4 64
- 8 128
- ½ 8
- ¼ 4
- 1/8 2
- 1/16 1
- Also:

2.Teilbarkeit

- Zahlenmuster (Rechteck)
- Z.B.12



2.1.Definition, Regeln

Es seien a, b Elemente der Menge **N**
(Kurzschreibweise: $a, b \in \mathbf{N}$, gelesen: „a und b aus **N**“).

a heißt ***Teiler*** von b genau dann, wenn die Gleichung $a \cdot x = b$ eine Zahl $x \in \mathbf{N}$ als Lösung besitzt.

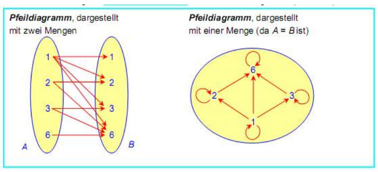
- Sprechweisen
- Schreibweise
- Begriffe: komplementärer Teiler, echte Teiler
- Beispiele
- Teilbarkeitsregeln
- Folgerungen
- Beweise

1. Für alle $a \in \mathbf{N}$ gilt $a \mid 0$.
2. Für alle $a \in \mathbf{N}^*$ gilt $0 \nmid a$.
3. Für alle $a \in \mathbf{N}$ gilt $1 \mid a$.
4. Für alle $a \in \mathbf{N}$ gilt $a \mid a$.
5. Für alle a Є **N*** gilt $a \mid b \Rightarrow a \le b$
6. Gilt d/a und d/b , so gilt auch d/(a+b)
7. Für alle n Є **N** gilt: Gilt d/a , so gilt auch d/(n*a)
8. Differenzregel

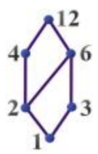
9.Produktregel

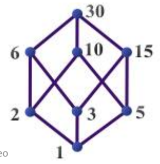
2.2.Teilbarkeitsrelation

- Pfeildiagramm



- Darstellung im Koordinatensystem
- Hasse-Diagramm





Ordnungsrelation

- geordnete Zahlenpaare in NxN

Transitiv

Die Teilbarkeitsrelation ist ***transitiv:*** Für alle $a,b,c \in \mathbf{N}$ gilt $(a, b) \in R$ und $(b, c) \in R \Rightarrow (a, c) \in R$.

Reflexiv Für alle a Є **N** gilt (a,a) Є R

Die Teilbarkeitsrelation ist ***identitiv:*** Für alle $a, b \in \mathbf{N}$ gilt $(a, b) \in R$ *und* $(b, a) \in R \Rightarrow a = b$.

Symmetrisch ?

2.3.Teilermengen

- Teilermenge = Menge aller Teiler

Es sei $a \in \mathbf{N}$. Die Menge aller Teiler von a,
d.h. die Menge $T_a = \{ t \in \mathbf{N}$, für die $t \mid a$ gilt $\}$ heißt ***Teilermenge von a***.
Bezeichnung: T_a oder T(a).

Beispiele: T(24)

- Aufzählend T(24)={1,2,3,4,6,8,12,24}
- Beschreibend

Fragen:

- Wie finde ich alle Teiler?
- Wieviele Teiler gibt es?

- T(0)=?
- Satz: Der Teiler a einer natürlichen Zahl n oder der komplementäre Teiler (n/a) sind kleiner oder gleich der Wurzel aus n.
- Beweis (indirekt)
- Beispiel T(504)

T(504)={1,2,3,4,6,7,8,9,12,14,18,21, }

Teileranzahlfunktion

$$d(n) = \tau(n) = \#\{d\colon 1 \leq d \leq n \text{ und } d \mid n\}.$$

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}, \quad d(n) = (e_1+1)(e_2+1)\cdots(e_r+1).$$

Für teilerfremde natürliche Zahlen m und n gilt $\tau(m \cdot n) = \tau(m) \cdot \tau(n)$

n	1	2	3	4	5	6	7	8	9	72	504	
Teiler												
Prim-teiler												101^3,103^2
d(n)												

Die Anzahl der Teiler einer natürlichen Zahl n hängt nicht von der Größe dieser Zahl ab, sondern von der Häufigkeit der Primteiler.

3.Primzahlen

- 3.1. Definition

Eine Zahl $p \in N^*$ heißt Primzahl, wenn sie genau zwei Teiler besitzt.

- T(p)={1,p}
- 1 ist keine Primzahl
- Teileranzahlfunktion d(p)=2

Der kleinste von 1 verschiedene Teiler jeder natürlichen Zahl ist eine Primzahl.

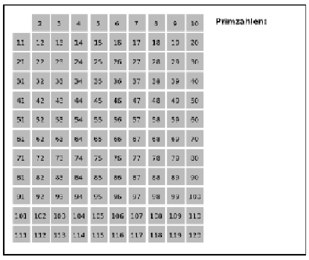
Eine Zahl $n \in N\backslash\{1\}$ heißt zusammengesetzte Zahl, wenn sie keine Primzahl ist.

3.2.Eigenschaften

- 2 ist die einzig gerade Primzahl
- Es gibt unendlich viele Primzahlen (Euler):
- Beweis: Sind $\mathbf{p_1}, \mathbf{p_2}, \ldots, \mathbf{p_r}$ die vorgelegten Primzahlen, so bildet man die neue Zahl $\mathbf{n = p_1 * p_2 * \ldots * p_r + 1}$. Diese natürliche Zahl **n** besitzt bis auf die Reihenfolge eine eindeutige Zerlegung in ihre Primfaktoren. Ist **q** einer der Primteiler von **n**, so kann er nicht unter den vorgelegten Primzahlen vorkommen, da jede der vorgelegten Primzahlen $\mathbf{p_1}, \mathbf{p_2}, \ldots, \mathbf{p_r}$ die Zahl **n** mit Rest 1 teilt und **q** als echter Teiler nicht. Somit ist **q** eine neue Primzahl und wegen diesem Widerspruch zur Annahme ist die Menge der Primzahlen unendlich.
  - Gibt es eine Formel?
- Primzahlzwillinge
- Drillinge

3.3. Bestimmung von Primzahlen

- Dividieren (0 Rest)
- Sieb des Eratosthenes



weitere Tests

- AKS-Primzahltest (2000)
- Fermatscher Primzahltest (probalistisch)

Der **kleine Fermatsche Satz:**

a^p Ξ a(mod p)

wobei *a* eine ganze Zahl und *p* eine Primzahl ist

- Glückliche Primzahlen
- http://primzahlen.zeta24.com/de/

3.3. Hauptsatz der Zahlentheorie

Jede natürliche Zahl n>1 besitzt (bis auf die Reihenfolge der Faktoren genau eine Primfaktorenzerlegung.

Beweis:
Existenz:

Der kleinste von 1 verschiedene Teiler jeder natürlichen Zahl ist eine Primzahl.

Eindeutigkeit: Indirekter Beweis

Primfaktorendarstellung

- Beispiele
  - 340 | 2
  - 170 | 2
  - 85 | 5
  - 17 | 17
- Normierte Primfaktorenzerlegung

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots\ldots \cdot p_r^{e_r} = \prod_{i=1}^{r} p_i^{e_i}$$

$$p_i \in P, n_i \in N^*$$

Zahlentheorie KPH Stams 25

Teilermenge

- Anzahl: $\tau(n) = (e_1 + 1) \cdot (e_2 + 1) \cdot \ldots \cdot (e_r + 1)$
- Teilermenge
  T(n) = Menge der Zahlen $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots\ldots \cdot p_r^{\alpha_r}$
- Beispiele: $(0 \le \alpha_i \le e_i)\, für \quad i = 1,2,\ldots,r$
  14=2*7
  T(14)=
  $18 = 2^1 \cdot 3^2$
  T(18)={

Zahlentheorie KPH Stams 26

Primzahlformeln

- $p = m^2 - 79 \cdot m + 1601$
- Satz: Es existiert kein Polynom, das für alle x Primzahlwerte annimmt
- Besondere Primzahlen
- Ungelöste Probleme
- Bedeutung

Zahlentheorie KPH Stams 27