

## Mathematik lebendig sehen – ein Stück Welt verstehen

Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 1

## Bézier-Splines [s p l a i n] angepasste Linie

Programm:  
GeoGebra  
frei!!!  
[www.geogebra.org](http://www.geogebra.org)

Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 2

## Hauptbahnhof Berlin Teil eines elliptischen Zylinders

Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 3

## Mathematik lebendig sehen – ein Stück Welt verstehen

Andalusien: parabolische Zylinder  
im Sonnenkraftwerk

Brennlinien  
mit Sonnenlicht  
am Kreis reflektiert:  
Katakaustiken

Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 4

## Konflikt-Graphen

Graphentheorie

Eine verkehrsmässige Einmündung

Die Verkehrsströme werden **Ecken**.  
Wenn zwei in Konflikt geraten,  
werden sie durch eine  
**Kante** verbunden.

**Eckenfärbung:** verschiedene  
Farben für „benachbarte“ Ecken

Gleiche Farbe:  
gemeinsam  
„Grün“

Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 5

## IBAN International Bank Account Number

DE 29 240 501 10 0063000400

Land Prüfzahl Bankleitzahl Konto 10-stellig

DE → 1314 Buchstabenstellung im Alphabet + 9

240 501 10 0063000400 1314 29

Teile diese Zahl durch 97

Der Rest muss **1** sein, sonst war die IBAN falsch.

Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 6

## Zugabe: Kryptografie

In der Ankündigung habe ich versprochen, dass Sie etwas zu diesem Thema erfahren.

Nun, ich bin vorbereitet, das Versprechen zu halten.

221797204671294268320361706002  
 908484257297815132912154134536  
 755579737713035436849042633739  
 70044742416586223123127841841  
 103834445923850528980795585067  
 343276628137979768790704027643  
 259967851255792128389796594248  
 023175029021226314569294054954  
 292836827319074885624864090786  
 794997965805138940056098246089

Die Nachricht wird in eine Zahl verwandelt, mit der Zahl wird „wild“ rechnet und dann gesendet. Nur der Empfänger zurückrechnen und dann lesen.

Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 25

## Diffie-Hellman-Schlüssel

$p=23$   
 $g=7$   
 $s=15$   
 $7^{15} \equiv_{23} 14$

$r=17$   
 $7^{17} \equiv_{23} 19$

$a=14$   
 $b=19$

$k = 19^{15} \equiv_{23} 20$

$k = 14^{17} \equiv_{23} 20$

Lies:  $7$  hoch  $15$  modulo  $23$  ist  $14$  und was heißt das ??????????

Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 26

## modulo-Potenzen

Lies:  $7$  hoch  $15$  modulo  $23$  ist  $14$  und was heißt das ??????????

Modul  $Z(23)$   
 $n=23$

$a=7$   
Bis zur 15-ten Potenz von 7  
 $k=15$

Ha 2010  
 $mod(a^k, n) = 14$

Potenzen von 7 in  $Z = \{1, 7, 49, 343, 2401, 16807, 117649, 823543, 5764801, 40353607, 282475249, 19773267, \dots\}$

Powers of 7 in  $Z(23) = \{1, 7, 3, 21, 9, 17, 4, 5, 12, 15, 13, 22, 16, 20, 2, 14\}$

Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 27

## modulo-Potenzen

Das war zum Verstehen, aber in Wahrheit sind die Zahlen riesig.

Primzahlen bei  $10^{200}$  Das Weltall enthält etwa  $10^{90}$  Atome

modulo 23

modulo 233

Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 28

## Diffie-Hellman-Schlüssel

Wenn „Mister X“ die ganze Kommunikation abfängt, also  $(p, g, a, b)$  hat, findet er dennoch nicht  $s, r$ .

Keine Chance!

Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 29

## Das waren jetzt die ganz hohen Gipfel!

189305275646015102432182045295415640595922740  
 0098778481272514561037626461679891407506620665  
 93284581358818052329010449494358683679059130  
 2000591144234006238722737595566457683634168958  
 7626164144676307968892001,990527615748121218  
 2046395411634058583224000987784812725145610376  
 2646167989140750662066593328455813588180523840  
 1044949435868367905913020005911442340062387227  
 375955664576836341689587626164144676477,1466534  
 74703394961591315618237046632010753334159183  
 1657522646862391806148286203565853292529865394  
 1017662500217072368122809304432913348637249331  
 7340940627002578382461504609394604166012943757  
 0438679462317222 Das sind  $p, g, a$ , kryptografisch echt.

Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 30