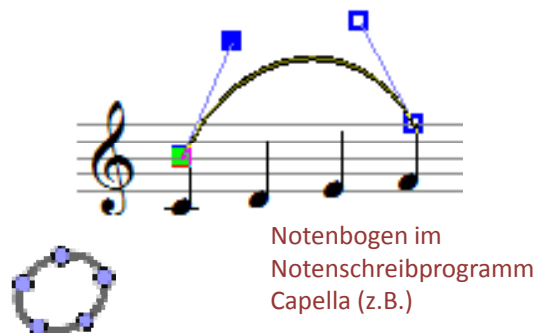


Mathematik lebendig sehen – ein Stück Welt verstehen



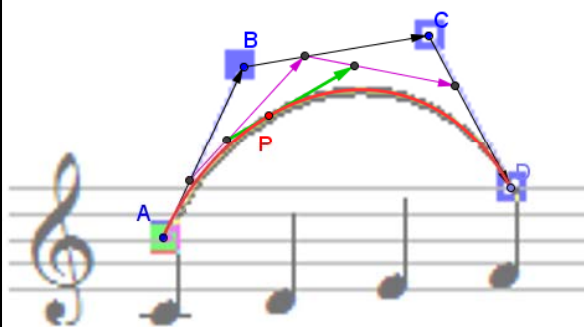
Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 1

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



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

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



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

Mathematik lebendig sehen – ein Stück Welt verstehen

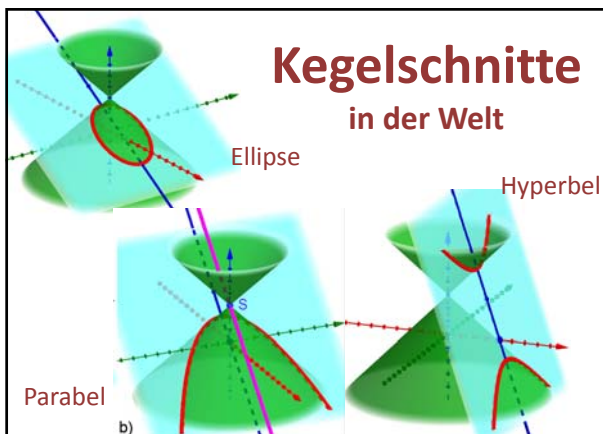
Kubische-Splines [s p l a i n] angepasste Linie minimale Biege-Energie



Strak-Latte

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

Kegelschnitte in der Welt



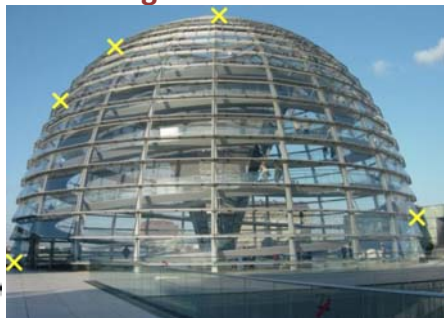
Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 5

Ellipsen und Kreise perspektivisch gesehen



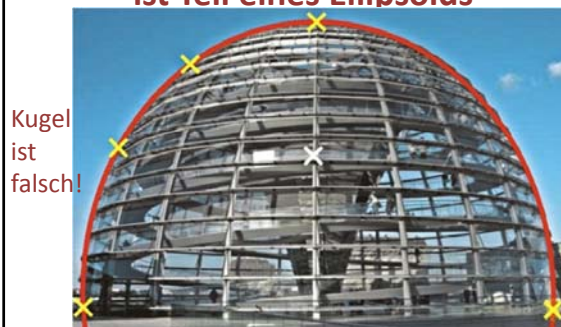
Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 6

Reichstagskuppel Berlin Teil einer Kugel? Oder doch nicht?



Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 7

Die Reichstagskuppel in Berlin ist Teil eines Ellipsoids



Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 8

Hauptbahnhof Berlin Teil eines elliptischen Zylinders



Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 9

Mathematik lebendig sehen – ein Stück Welt verstehen



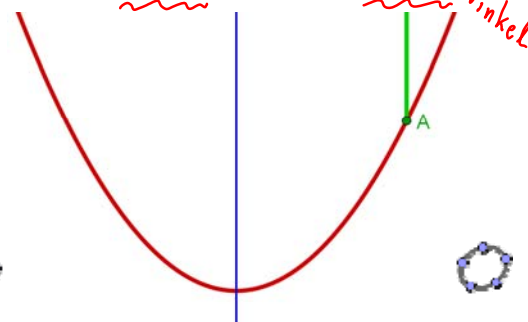
Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 10

Kein Kurpark ohne Parabeln



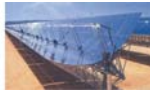
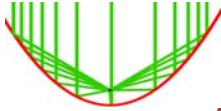
Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 11

Reflexion hat ein Gesetz: Einfallspinsel = Ausfallspinsel *Winkel*

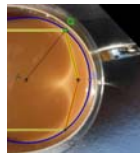


Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 12

Mathematik lebendig sehen – ein Stück Welt verstehen



Andalusien: parabolische Zylinder
im Sonnenkraftwerk



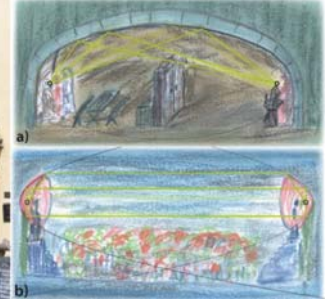
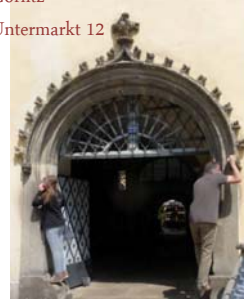
Brennlinien
mit Sonnenlicht
am Kreis reflektiert:
Katakaustiken

Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 13

Reflexion an Ellipsen und Parabeln Flüstergewölbe, Flüsterschalen

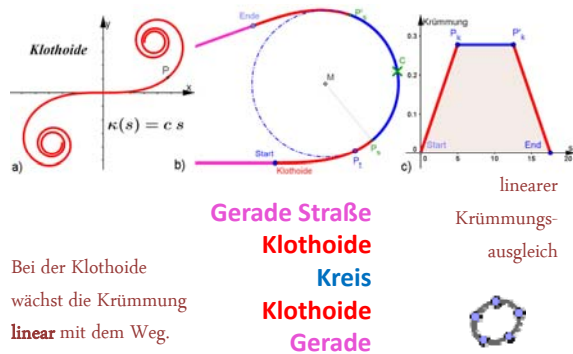
Görlitz

Untermarkt 12



Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 14

Keine Straße ohne Klothoide



Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 15

Den Goldenen Schnitt lebendig sehen

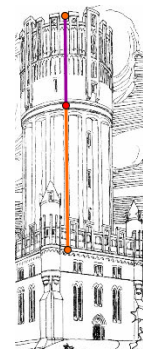


Abb. 5.38 Blattansätze mit 61,8 %, 60 % und 62,5 % des Vorblatts

Abb. 5.39 Der Blattansatz geschieht im goldenen Winkel

Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 16

EAN Europäische Artikelnummer



Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 17

EAN Europäische Artikelnummer



EAN 1 234 567 891 234

Produkte 11, 6, 3, 12, 5, 18, 7, 24, 9, 3, 2, 9, 4)

Prüfsumme 103 passt nicht, es muss ein voller Zehner sein

ISBN10 "1234567897"

Ergebnis:

Produkte (10, 18, 24, 28, 30, 30, 28, 24, 18, 7)
Prüfsumme ISBN10 217 passt nicht, nächster Elfer ist 220
Die neue Buchnummer ist ISBN13 = 9781234567897

Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 18

IBAN International Bank Account Number

DE 29 240 501 10 0063000400

Land Prüfnzahl 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 19

IBAN International Bank Account Number

IBAN berechnen und prüfen Haftendorn 2013, Info aus www.iban.de

Berechnung der IBAN

$bkl = 24050110 + 24050110$

$kto = 63000400 + 63000400$

Deutschland DE wird 1314. Weil D die 4. und 5. Buchstaben in

zu diesen Plätzen 9 addiert wird. $la = 1314 + 1314 \text{ land} = "DE" + DE$

$zahl = bkl \cdot 10^{16} + kto \cdot 10^6 + la \cdot 100 + 240501100063000400131400$

$zm = \text{mod}(zahl, 97) = 69 \quad pr = 98 - zm = 29$ Das sind die Prüfziffern

$ibanliste = \{ \text{land}, pr, bkl \cdot 10^{10} + kto \} \cdot ibanliste = \{ "DE", 29, 240501100063000400 \}$

Deutsche IBAN prüfen: $la = 1314$ Für andere Länder s. o.

Trage ein die Zahl hinter den Landesbuchstaben ein: $ibanpr = 29240501100063000400$ Hänge

$la = 1314$ an.

$prp = \text{floor} \left(\frac{ibanpr}{10^{18}} \right) = 29$ Das wird vorn weggenommen und ganz hinten angehängt.

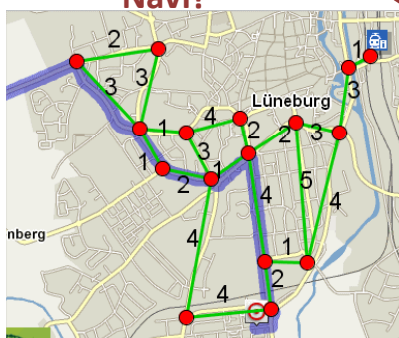
$zahlp = \text{mod}(ibanpr, 10^{18}) \cdot 10^6 + la \cdot 100 + prp$

$\text{mod}(zahlp, 97) = 1$ Wenn hier nicht 1 steht, die die IBAN falsch.

Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 20

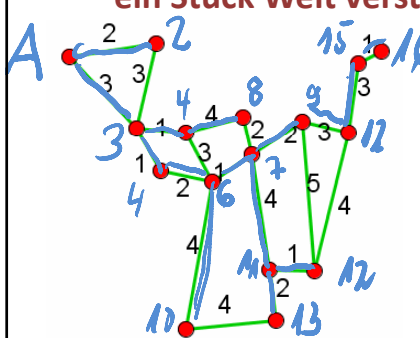
Wie arbeitet das Navi?

Graphentheorie



Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 21

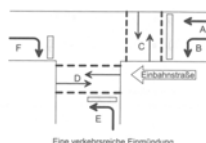
Mathematik lebendig sehen – ein Stück Welt verstehen



Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 22

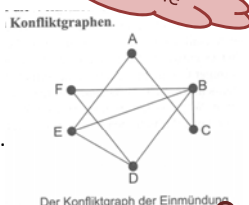
Konflikt-Graphen

Graphentheorie



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

Eckenfärbung: verschiedene
Farben für „benachbarte“ Ecken



Der Konfliktgraph der Einmündung

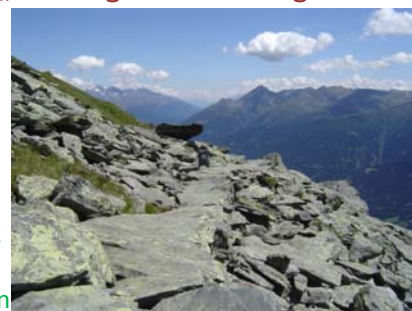
Gleiche Farbe:
gemeinsam
„Grün“

Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 23

Osttirol mit „Venediger-Höhenweg“

Eine schroffe
steinige Welt
gangbar
gemacht vom
Alpenverein.

Als Alpenverein
der Mathematik
habe ich Sie
hoffentlich einen
gangbaren Weg
geführt.



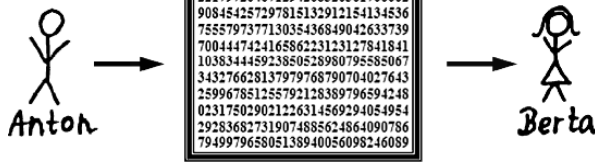
Vielen Dank für Ihre Aufmerksamkeit

Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 24

Zugabe: Kryptografie

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

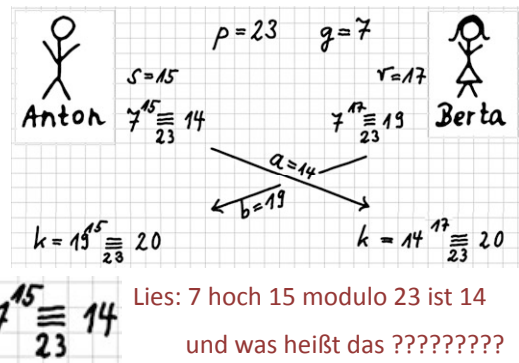
Nun, ich bin vorbereitet, das Versprechen zu halten.



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

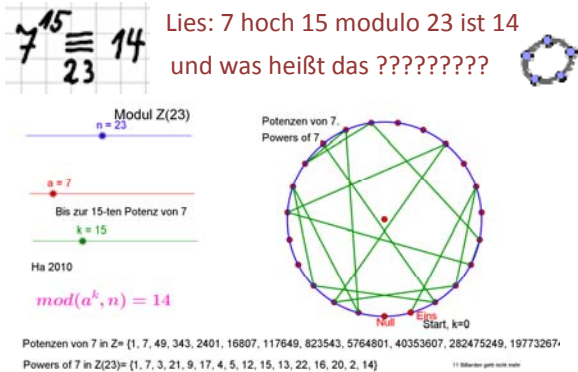
Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 25

Diffie-Hellman-Schlüssel



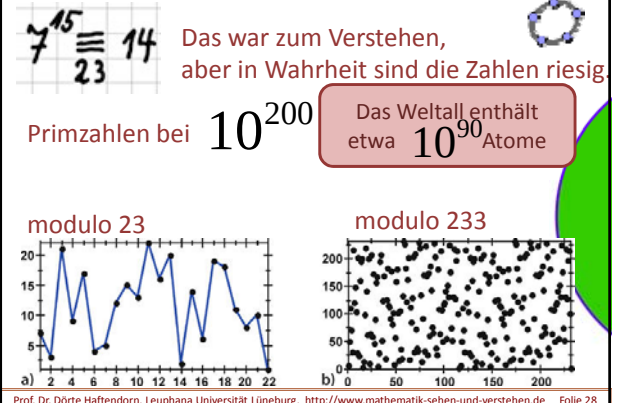
Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 26

modulo-Potenzen



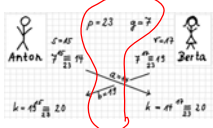
Prof. Dr. Dörte Haftendorn, Leuphana Universität Lüneburg, <http://www.mathematik-sehen-und-verstehen.de> Folie 27

modulo-Potenzen



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!**

18990527646045102432189294639541564059592240
0098778481272514561037626461679891407906620665
9313845581358813052329010449494358683679059130
2000591144234006238722737595566457683634168958
7626164144676307968892001,990527813746834121218
2046395411634058583224000987784812725145610376
2646167989140750662066593328455813588180523840
1044949435868367905913020005911442340062387227
375955664576836341689587626164144676477,1466534
747033949659913155182370366320207523341359183
1657522646862391806148286203565853292529865394
1017662500407072258432800394432913388637249331
7340940627002578582461504609394604166012943757
0438679462317222 Das sind p, g, a , kryptografisch echt.

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

■ Diffie-Hellman-Schlüsselvereinbarung

Haftendorn 2016

```
In[16]:= p = NextPrime[11^200]  
          |  
          | nächste Primzahl
```

```
Out[16]= 18 990 527 646 046 182 421 218 204 639 541 163 405 858 322 400 098 778 481 272 514 561 037 626 461 679 \  
          891 407 506 620 665 933 284 558 135 881 805 238 401 044 949 435 868 367 905 913 020 005 911 442 340 \  
          062 387 227 375 955 664 576 836 341 689 587 626 164 144 676 307 968 892 791
```

```
In[17]:= PrimeQ[p]  
          |  
          | Primzahl?
```

```
Out[17]= True
```

```
In[20]:= g = NextPrime[234 p]  
          |  
          | nächste Primzahl
```

```
Out[20]= 4 443 783 469 174 806 686 565 059 885 652 632 236 970 847 441 623 114 164 617 768 407 282 804 592 033 \  
          094 589 356 549 235 828 388 586 603 796 342 425 785 844 518 167 993 198 089 983 646 681 383 277 507 \  
          574 598 611 205 973 625 510 979 703 955 363 504 522 409 854 256 064 720 913 611
```

Erzeugung der Sendung Anton

```
In[22]:= s = 25 048; a = PowerMod[g, s, p]  
          |  
          | Potenz Modulo
```

```
Out[22]= 6 306 029 392 606 924 557 544 155 479 457 722 063 244 072 710 499 192 495 693 501 904 850 787 678 598 \  
          822 831 518 102 184 584 696 208 528 996 033 751 252 719 301 039 958 140 101 826 030 696 926 919 435 \  
          136 344 053 835 183 093 302 920 476 055 729 855 099 637 663 338 015 161 789
```

Erzeugung der Sendung Berta

```
In[23]:= r = 280 129; b = PowerMod[g, r, p]  
          |  
          | Potenz Modulo
```

```
Out[23]= 3 189 718 080 740 502 493 143 062 528 762 913 766 447 443 711 090 962 397 677 145 434 864 820 323 495 \  
          692 979 457 806 920 944 029 998 488 249 868 371 366 178 357 799 488 980 241 146 415 384 794 697 296 \  
          418 176 842 629 082 931 146 846 981 165 472 379 560 350 442 160 795 481 949
```

Die beiden Schlüssel:

```
In[25]:= anton = PowerMod[b, s, p]  
          |  
          | Potenz Modulo
```

```
Out[25]= 1 123 533 345 367 848 854 388 561 138 869 724 414 721 581 321 646 759 142 253 479 651 093 700 198 175 \  
          119 455 415 281 845 324 418 626 275 270 491 712 754 321 413 570 777 226 367 330 843 499 755 865 739 \  
          617 543 925 305 989 926 413 784 429 582 974 270 840 018 296 358 651 048 003
```

```
In[26]:= berta = PowerMod[a, r, p]  
          |  
          | Potenz Modulo
```

```
Out[26]= 1 123 533 345 367 848 854 388 561 138 869 724 414 721 581 321 646 759 142 253 479 651 093 700 198 175 \  
          119 455 415 281 845 324 418 626 275 270 491 712 754 321 413 570 777 226 367 330 843 499 755 865 739 \  
          617 543 925 305 989 926 413 784 429 582 974 270 840 018 296 358 651 048 003
```

```
In[27]:= anton - berta
```

```
Out[27]= 0
```