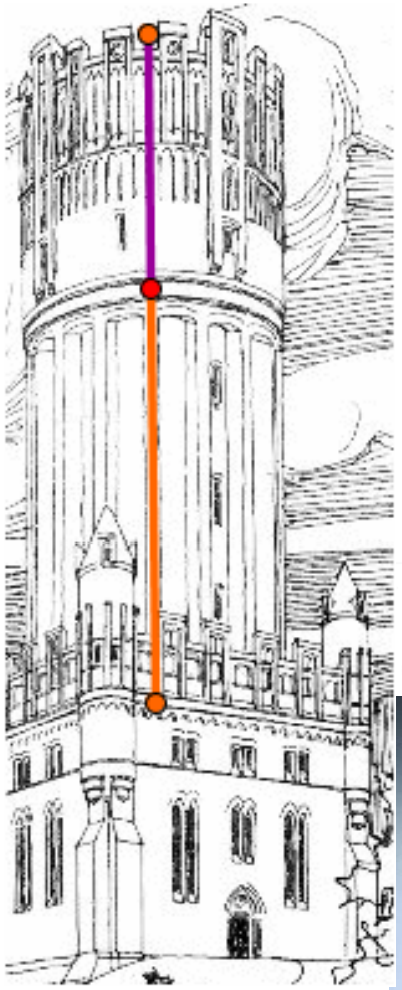
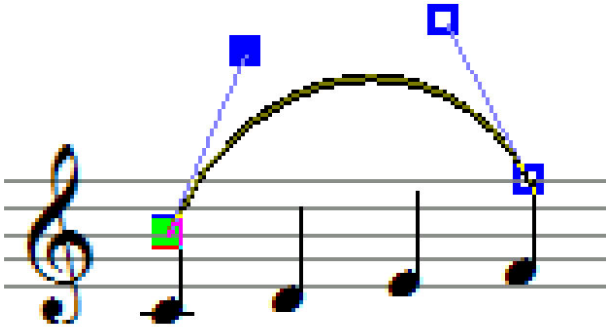
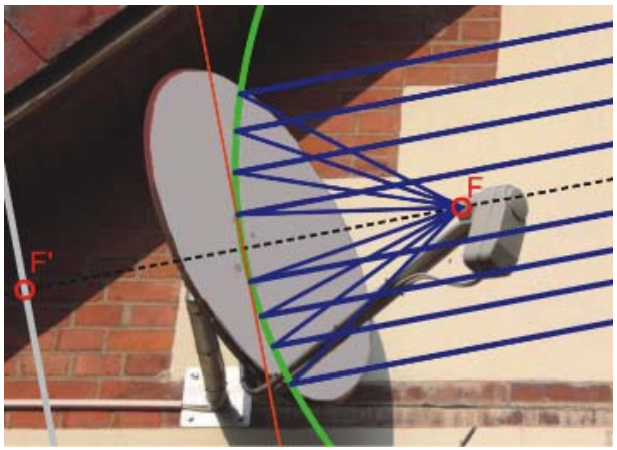
Mathematik lebendig sehen – ein Stück Welt verstehen

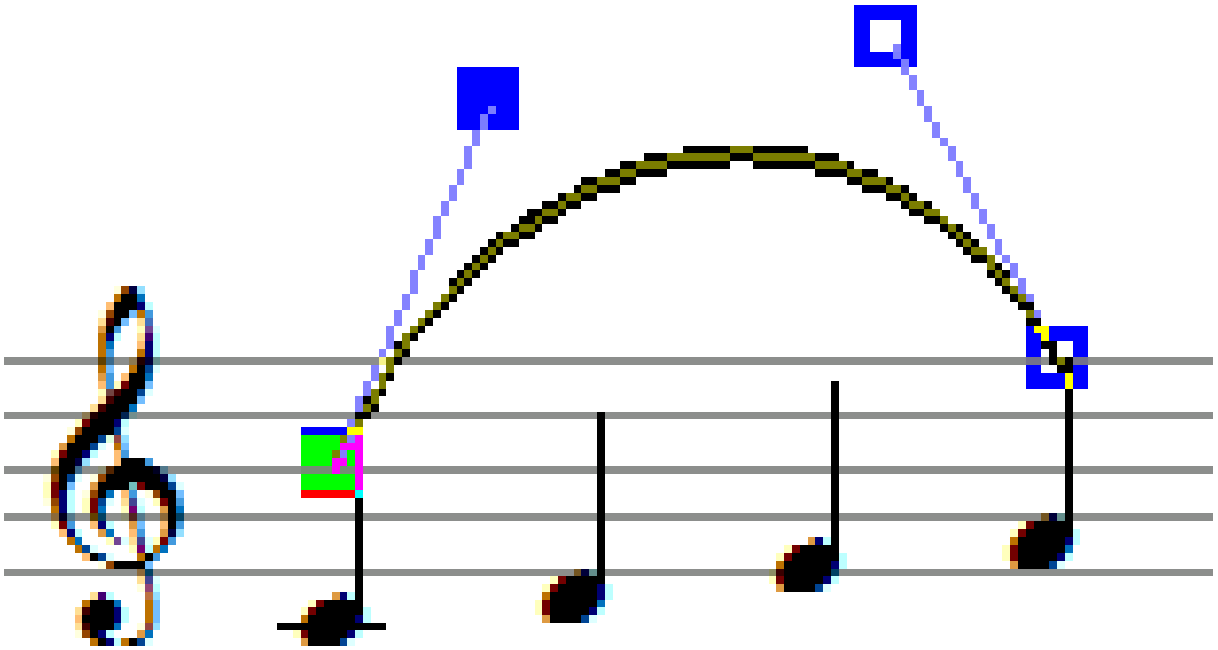


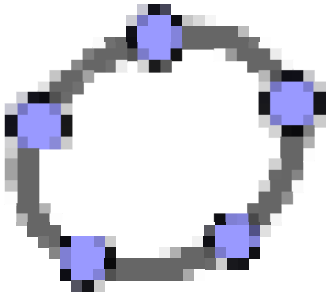




Bézier-Splines

[s p l a i n]
angepasste Linie

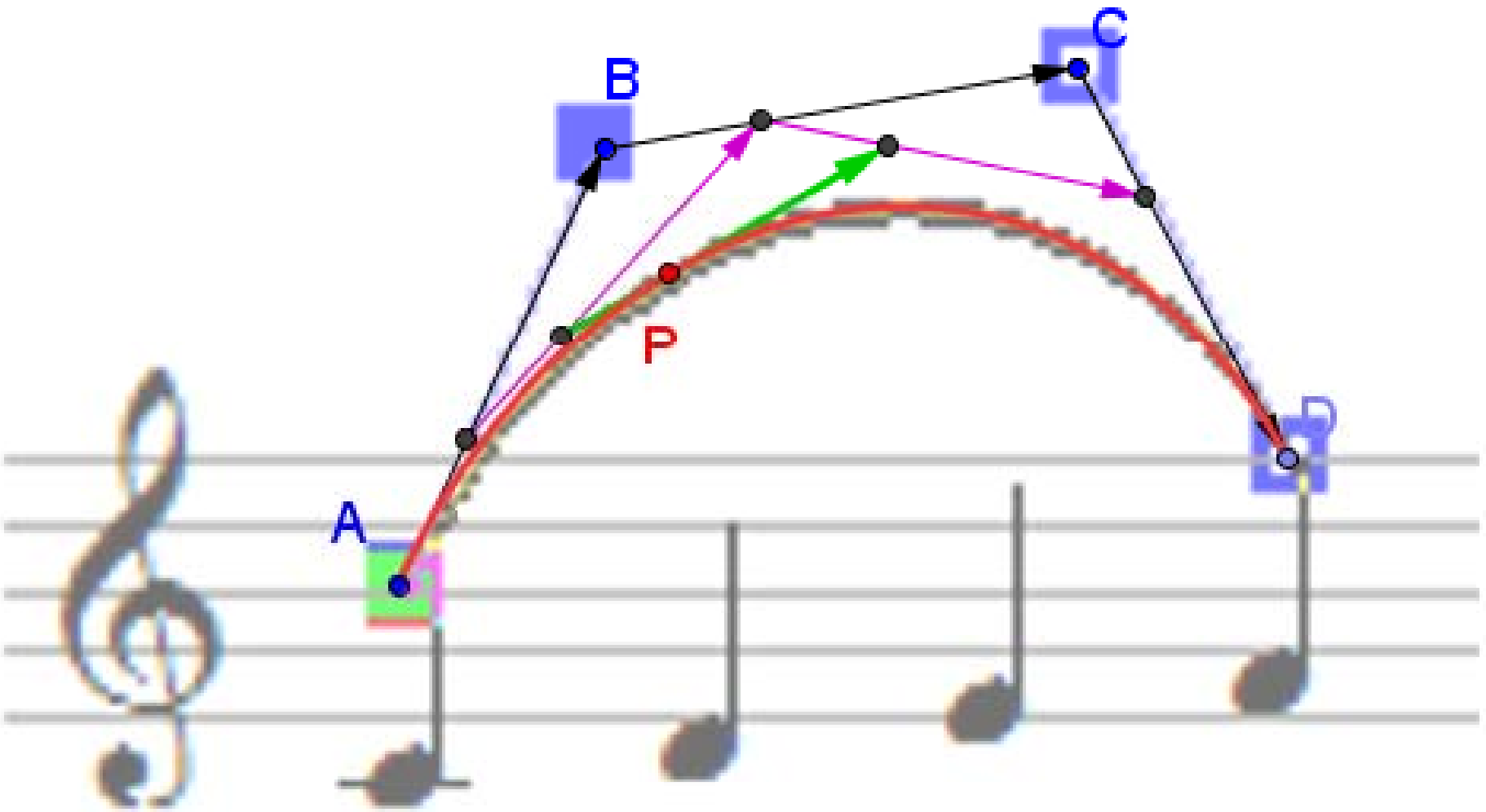




Notenbogen im
Notenschreibprogramm
Capella (z.B.)

Bézier-Splines

[s p l a i n]
angepasste Linie



Mathematik lebendig sehen – ein Stück Welt verstehen

Kubische-Splines

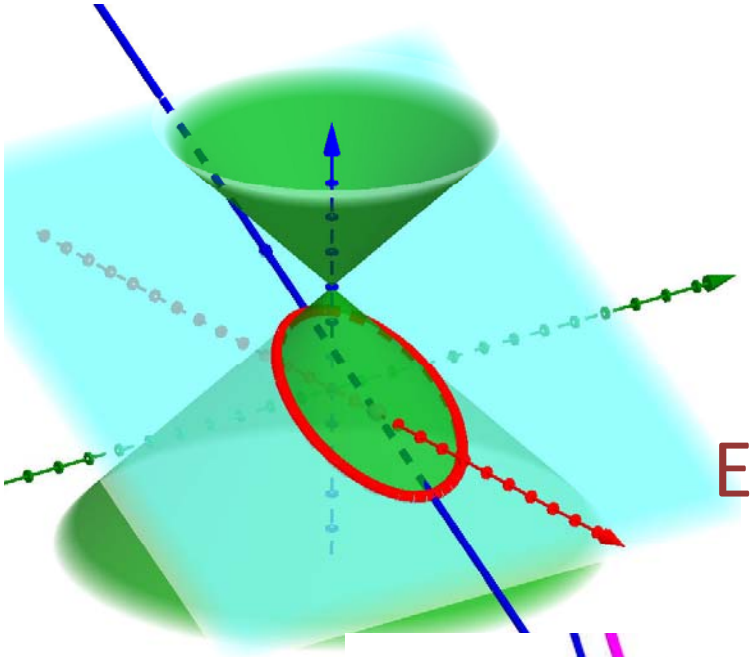
[s p l a i n] angepasste Linie

minimale Biege-Energie

Strak-Latte

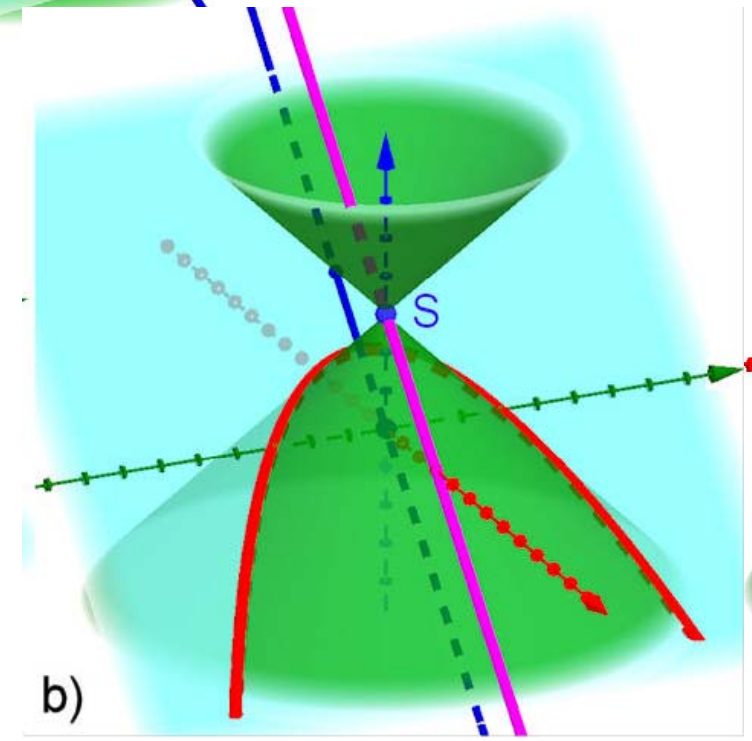
Kegelschnitte

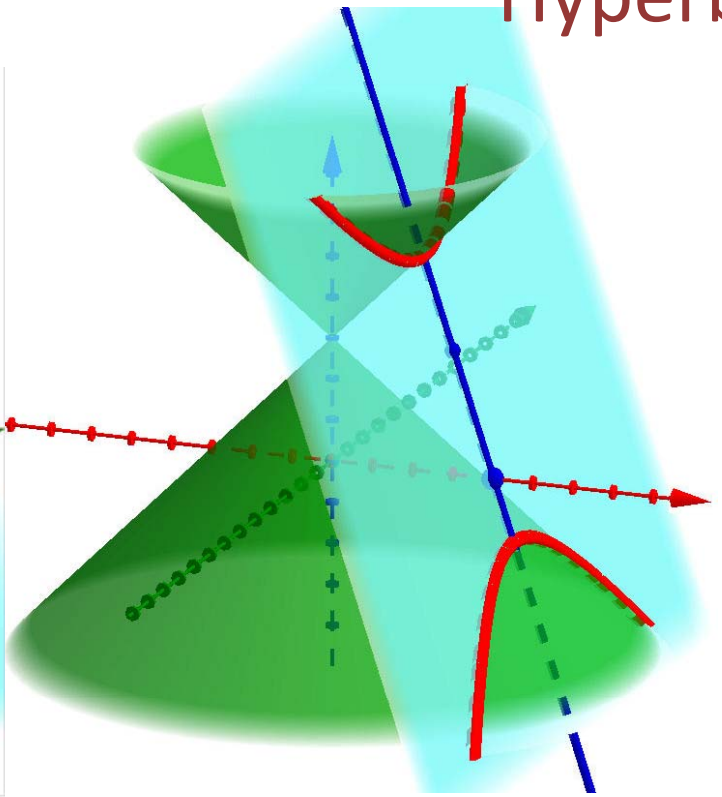
in der Welt



Ellipse

Hyperbel



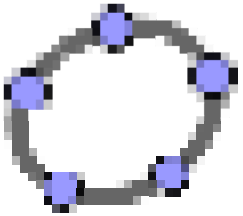


Parabel

Ellipsen und Kreise

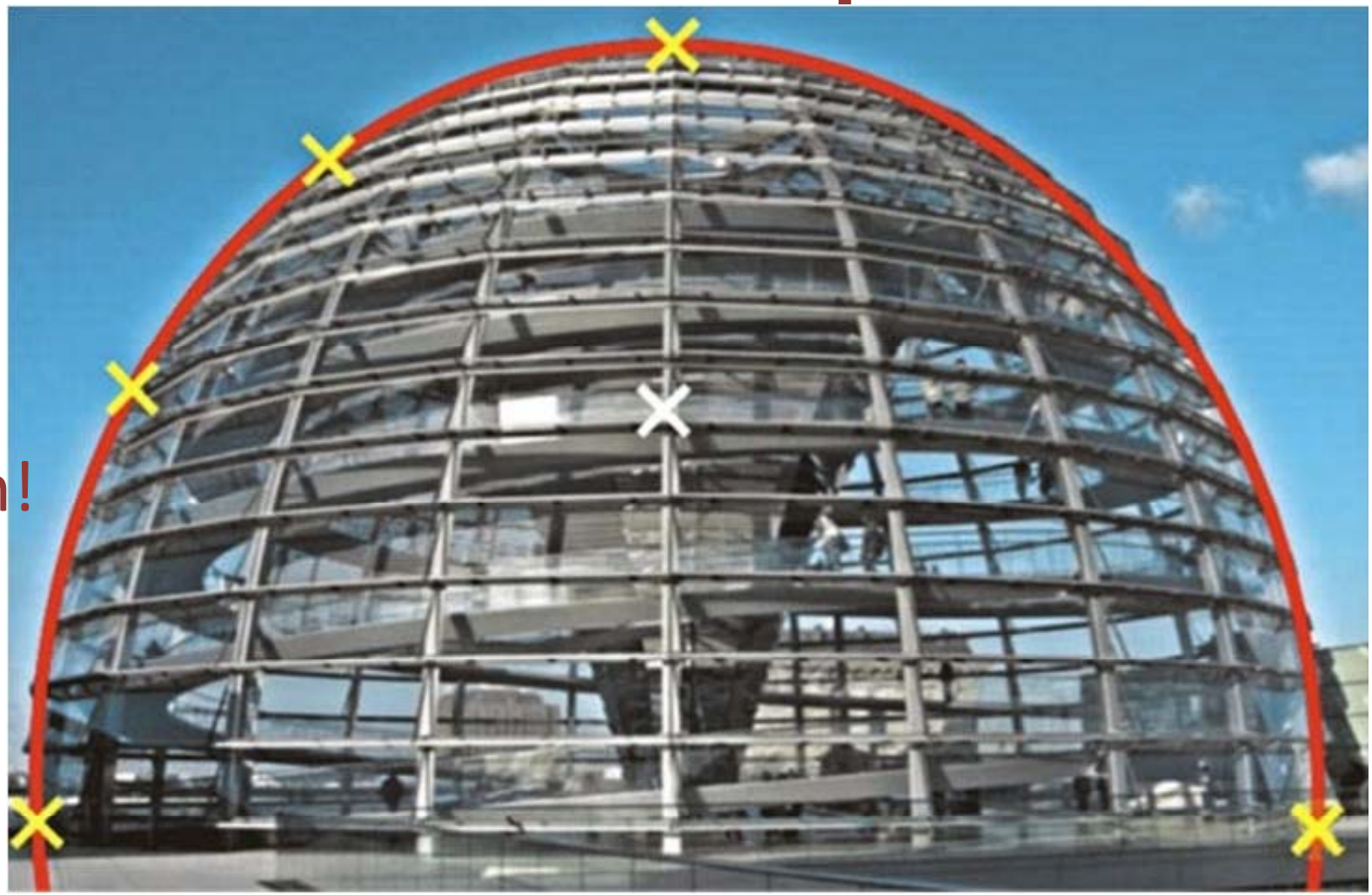
perspektivisch gesehen

Reichstagskuppel Berlin
Teil einer Kugel? Oder doch nicht?

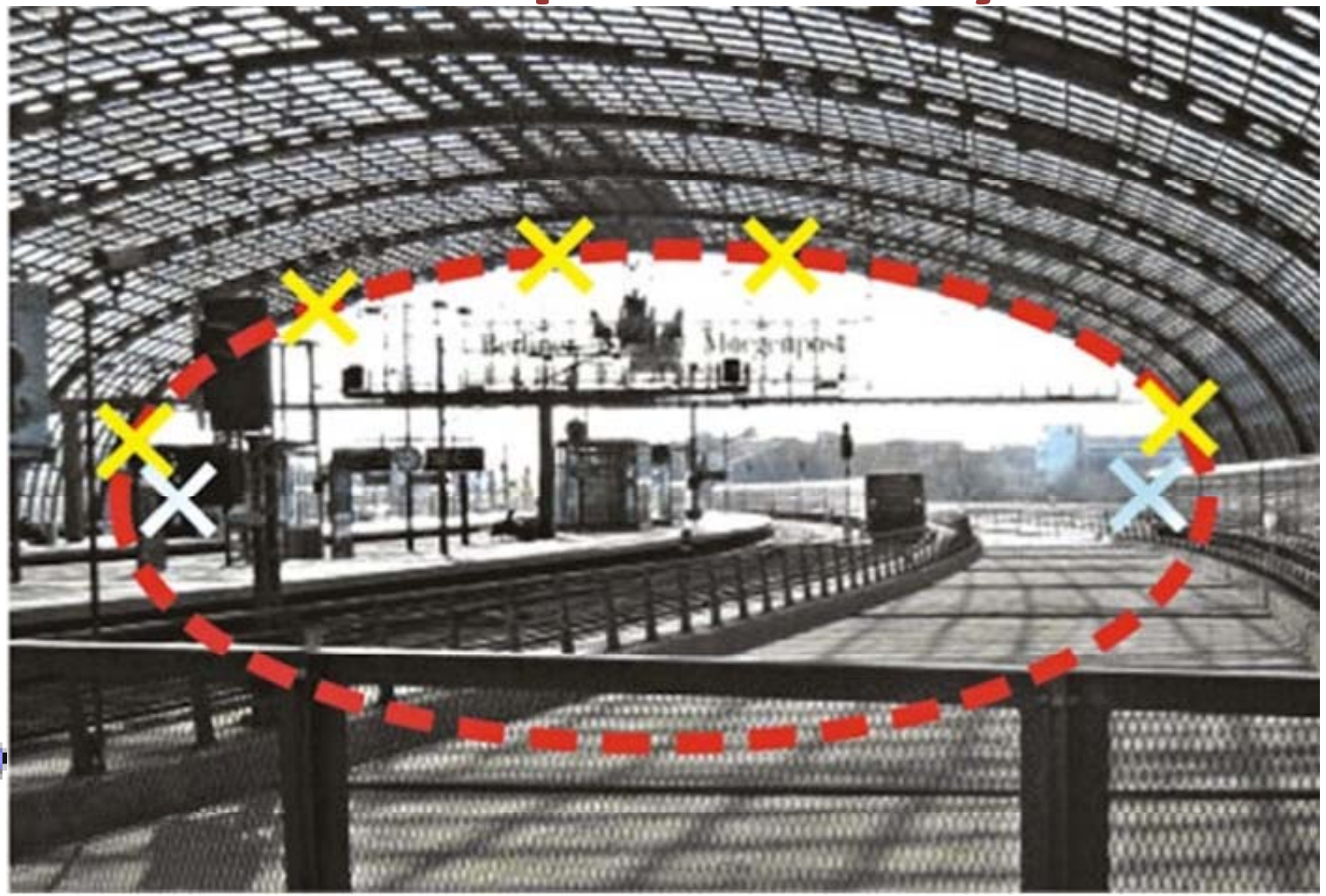


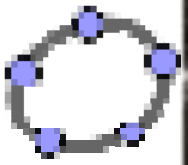
Die Reichstagskuppel in Berlin ist Teil eines Ellipsoids

Kugel ist falsch!



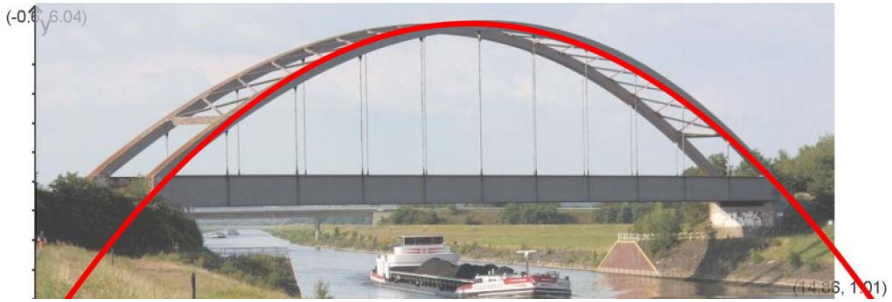
Hauptbahnhof Berlin
Teil eines elliptischen Zylinders



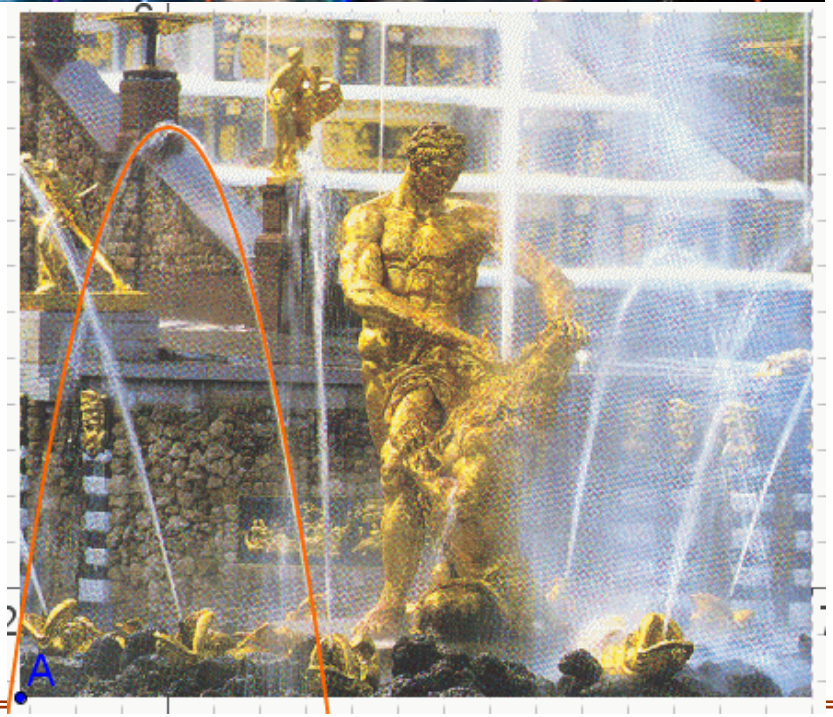


Mathematik lebendig sehen – ein Stück Welt verstehen

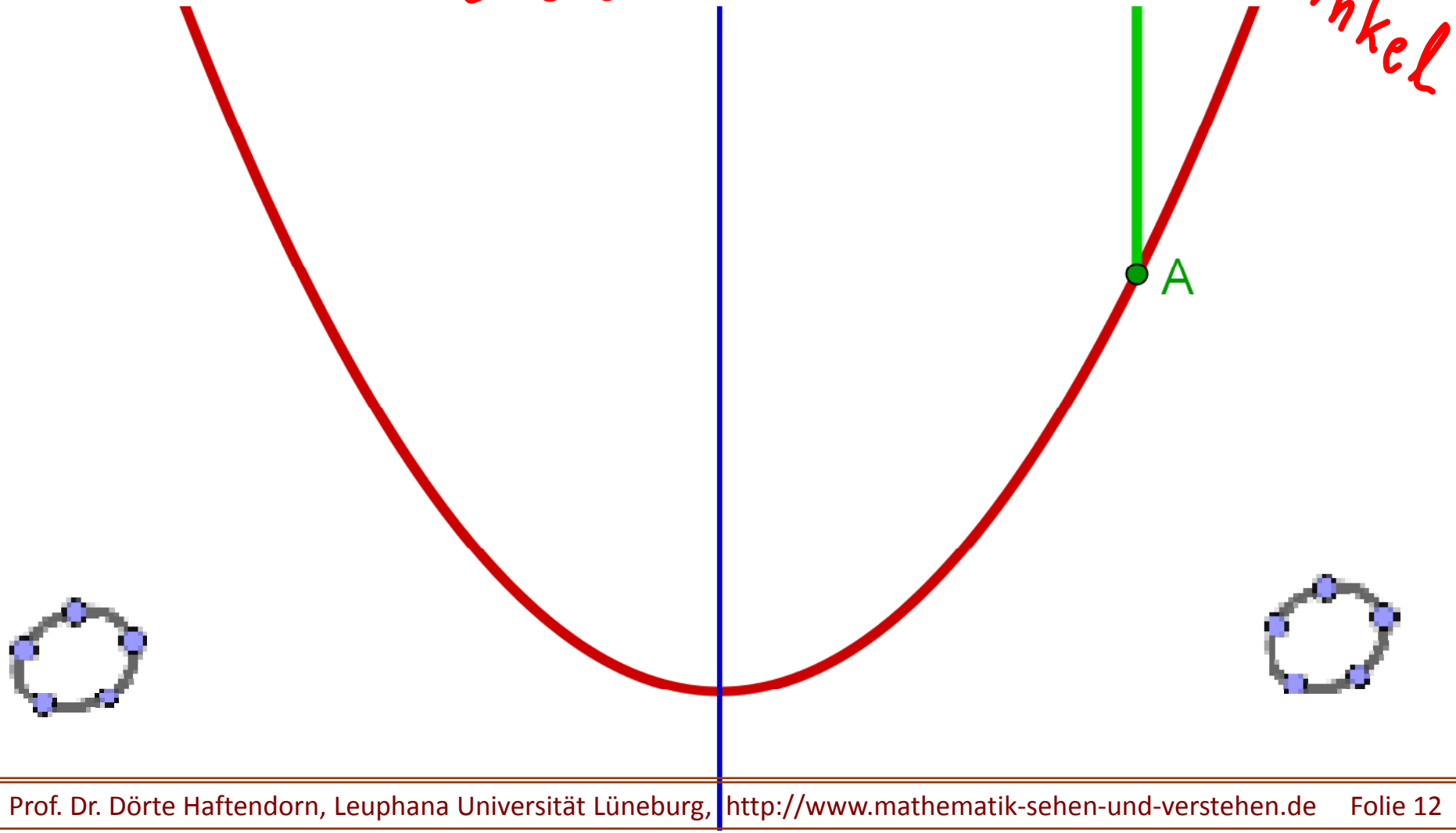
Brücke der Bahn über den Elbeseitenkanal am Inselsee



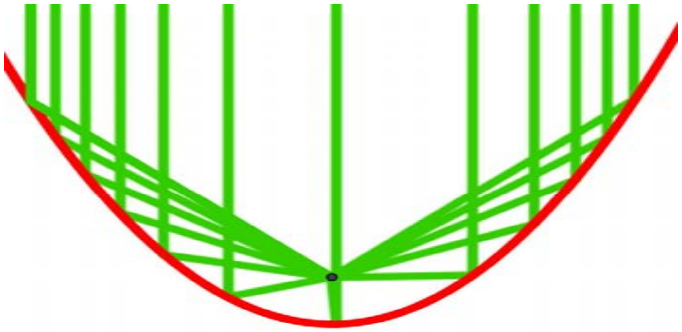
Kein Kurpark ohne Parabeln

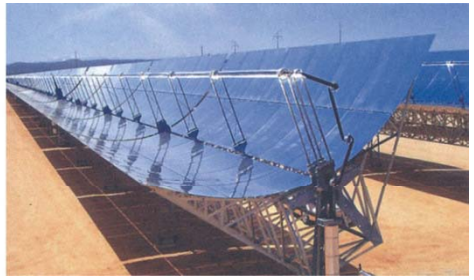


Reflexion hat ein Gesetz:
Einfallspinsel = Ausfallspinsel

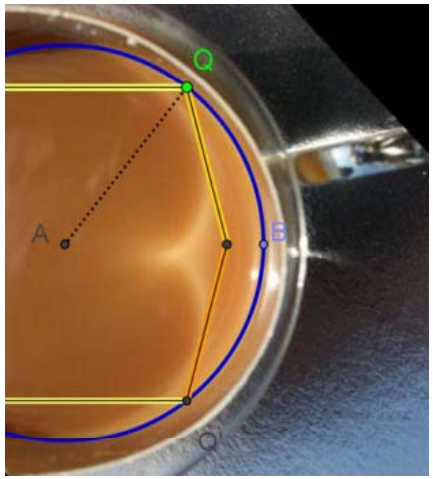


Mathematik lebendig sehen – ein Stück Welt verstehen





Andalusien: parabolische Zylinder im Sonnenkraftwerk

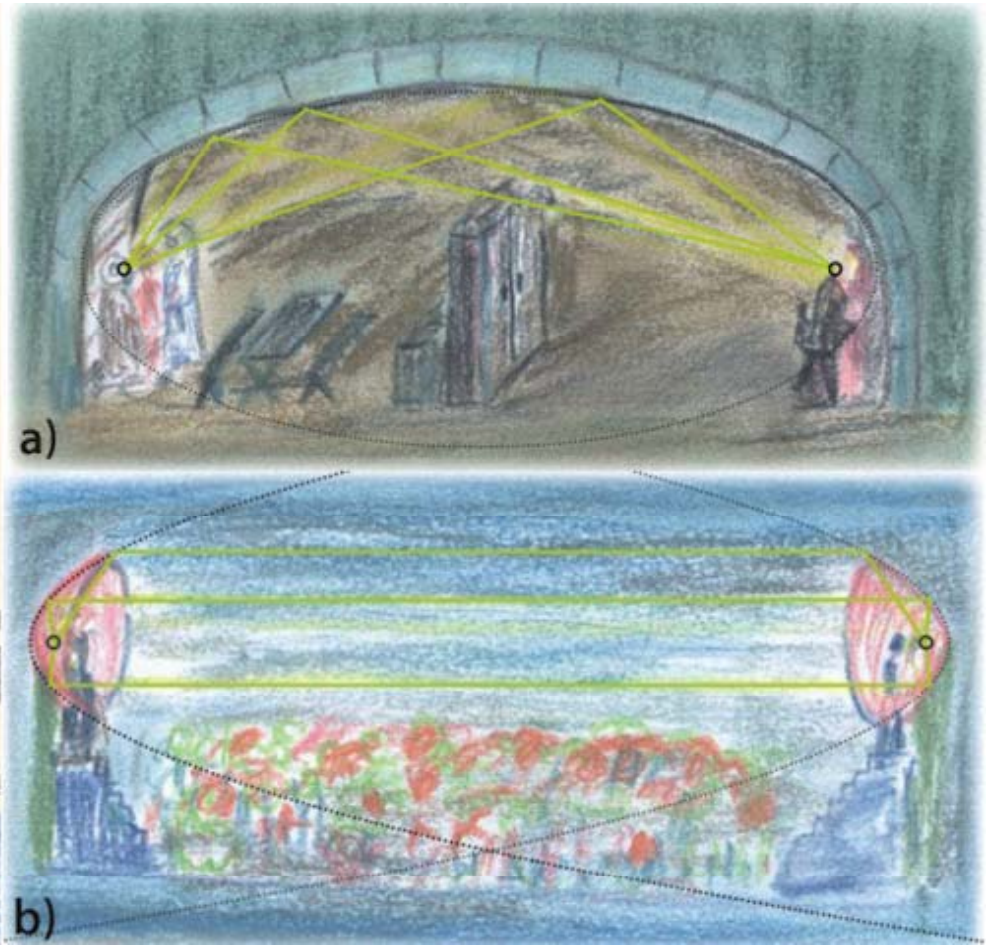


Brennlinien mit Sonnenlicht am Kreis reflektiert: Katakaustiken

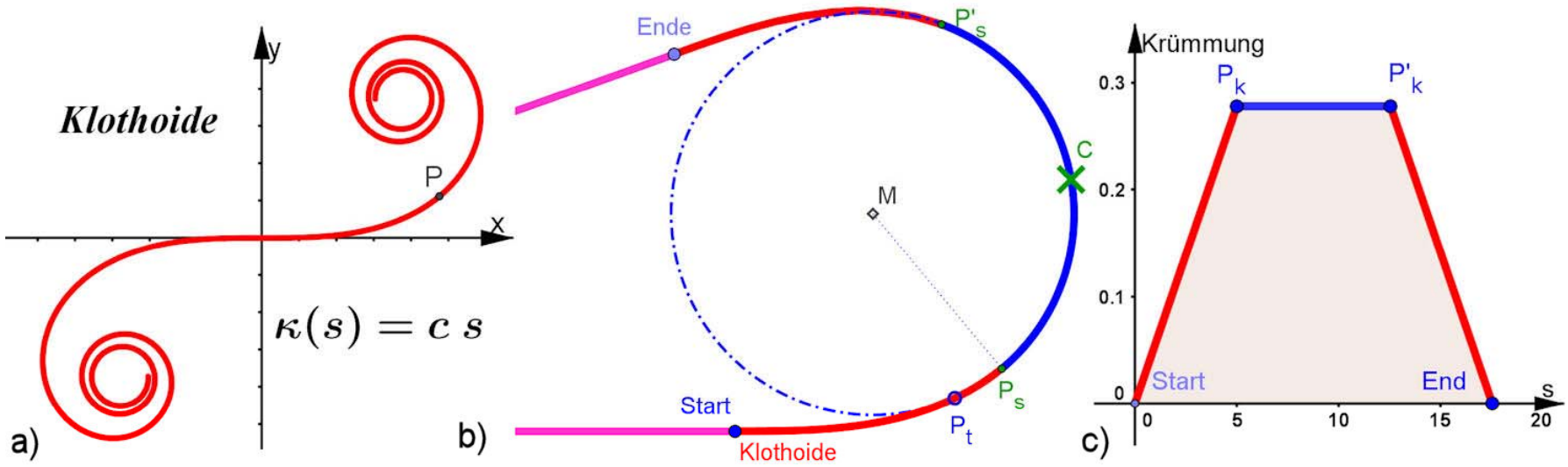
Reflexion an Ellipsen und Parabeln
Flüstergewölbe, Flüsterschalen

Görlitz

Untermarkt 12



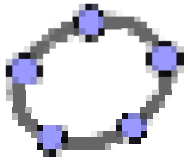
Keine Straße ohne Klothoide



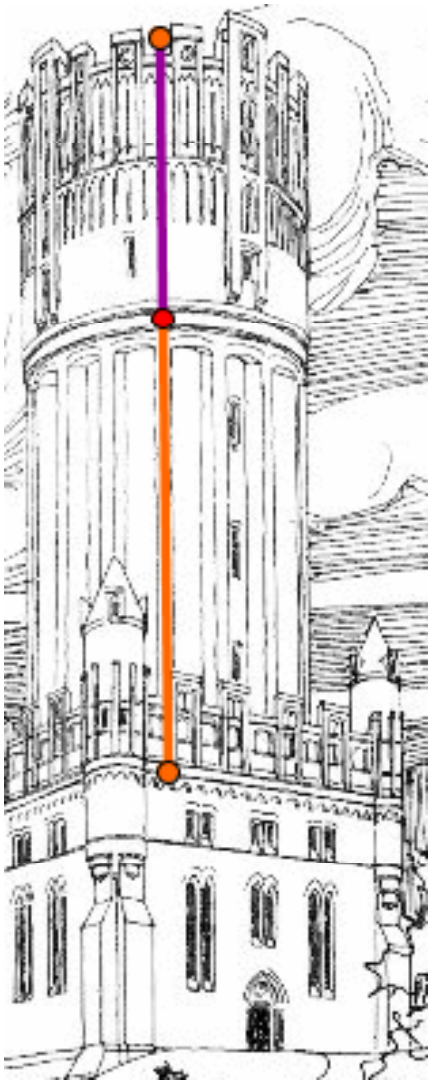
Bei der Klothoide
wächst die Krümmung
linear mit dem Weg.

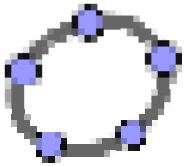
Gerade Straße
Klothoide
Kreis
Klothoide
Gerade

linearer
Krümmungs-
ausgleich



Den Goldenen Schnitt lebendig sehen





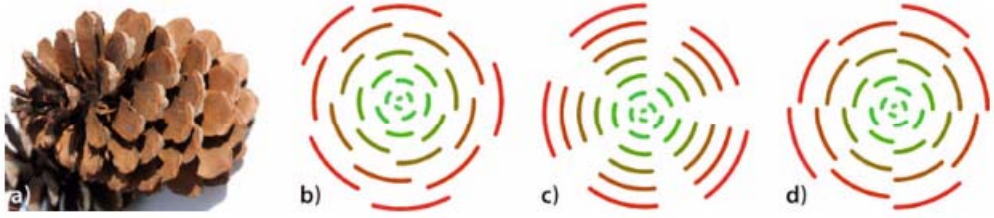


Abb. 5.38 Blattansätze mit 61,8 %, 60 % und 62,5 % des Vollwinkels

Abb. 5.39 Der Blattansatz geschieht im goldenen Winkel

EAN Europäische Artikelnummer

+25 → ·3 → 75 → 100 ok

EAN Europäische Artikelnummer

+25 → ·3 → 75 → 100 ok

+25

EAN 1 234 567 891 234

```
Produkte
{1, 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                         passt nicht, nächster Elfer ist
217                                     220
Die neue Buchnummer ist ISBN13 =        9 781 234 567 897
```

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.

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 und E die 4. und 5. Buchstaben ir

zu diesen Plätzen 9 addiert wird. **la**:=1314 ▸ 1314 **land**:="DE" ▸ DE

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

zm:=mod(**zahl**,97) ▸ 69 **pr**:=98−**zm** ▸ 29 Das sind die Prüfziffern

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

Deutsche IBAN prüfen: **la** ▸ 1314 Für andere Länder s.o.

Trage ein die Zahl hinter den Landesbuchstaben ein: **ibanp**:=292405011000063000400 Hänge **la** ▸ 1314 an.

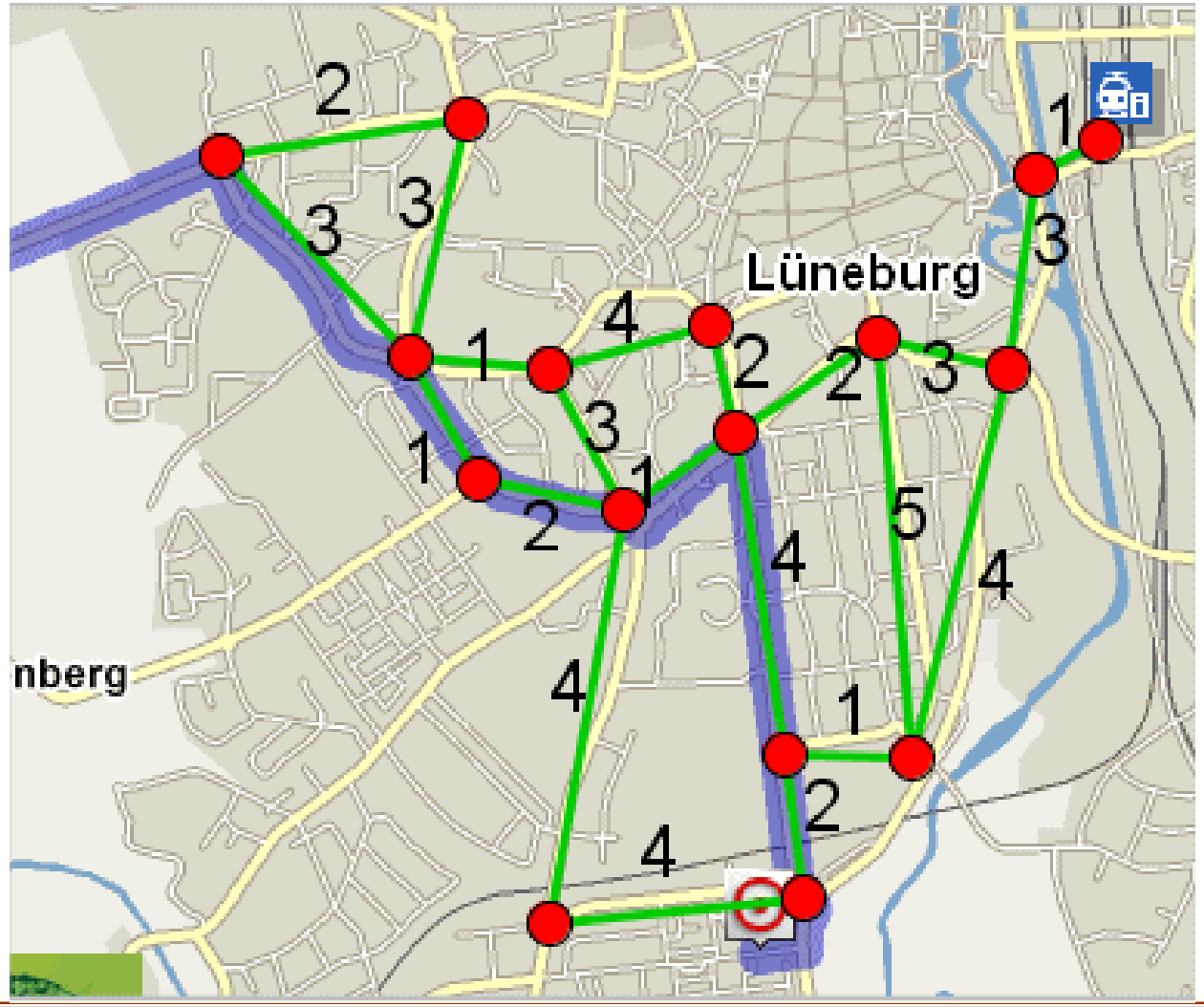
$$\mathbf{prp}:=\mathrm{floor}\left(\frac{\mathbf{ibanp}}{10^{18}}\right) \blacktriangleright 29$$ Das wird vorn weggenommen und ganz hinten angehängt.

zahlp:=mod(**ibanp**,10^{18})$\cdot 10^{6}$+**la**$\cdot 100$+**prp**

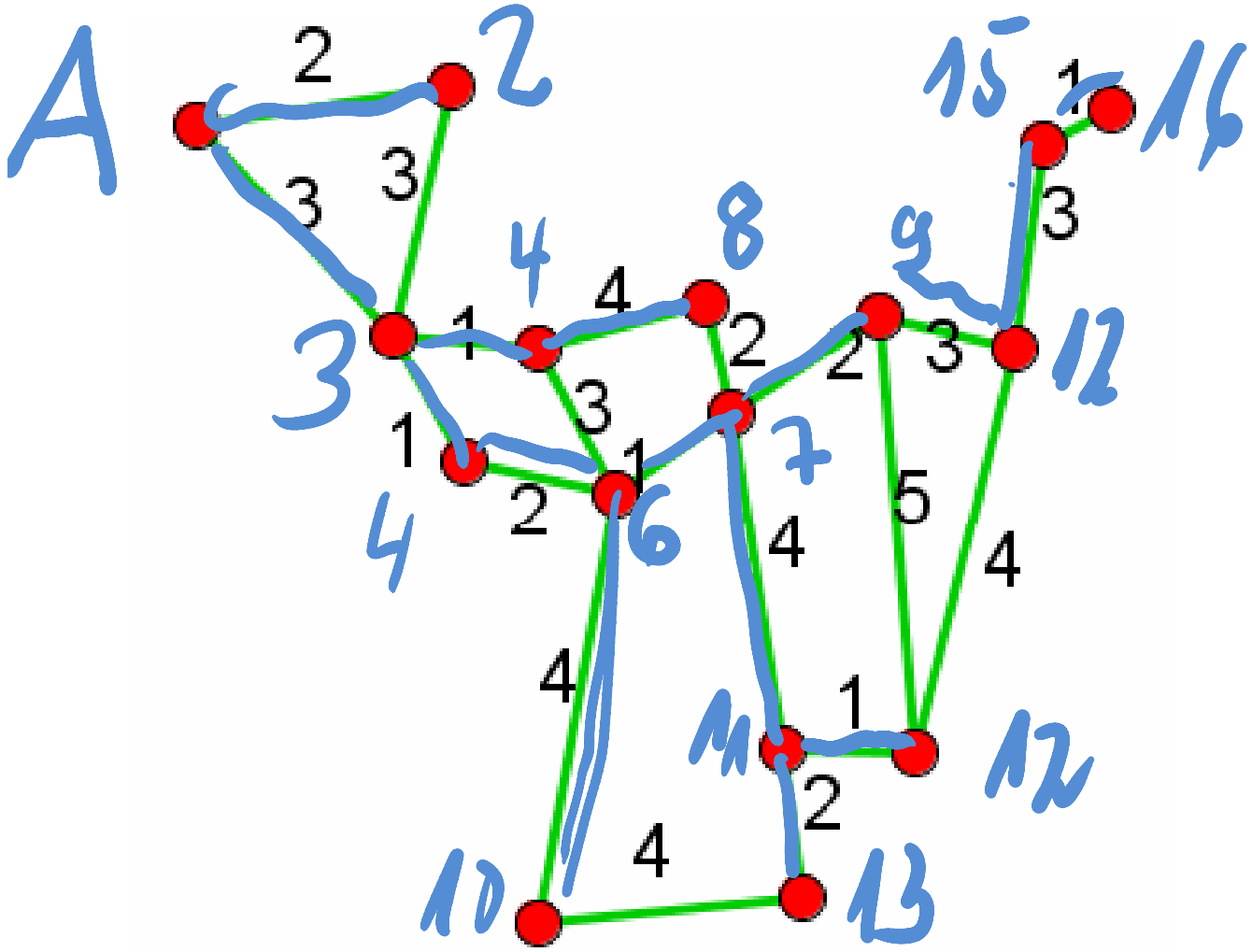
mod(**zahlp**,97) ▸ 1 **Wenn hier nicht 1 steht, die die IBAN falsch**.

Wie arbeitet das Navi?

Graphentheorie

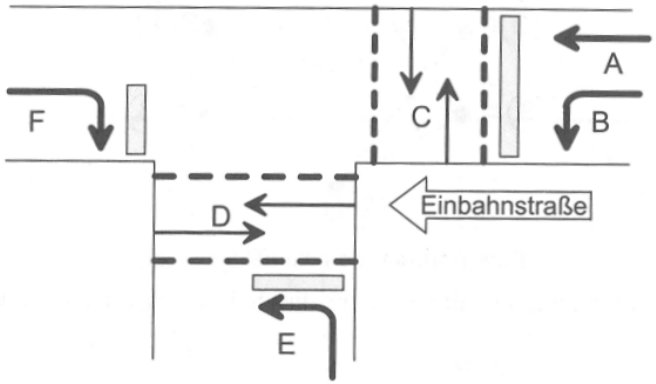


Mathematik lebendig sehen – ein Stück Welt verstehen



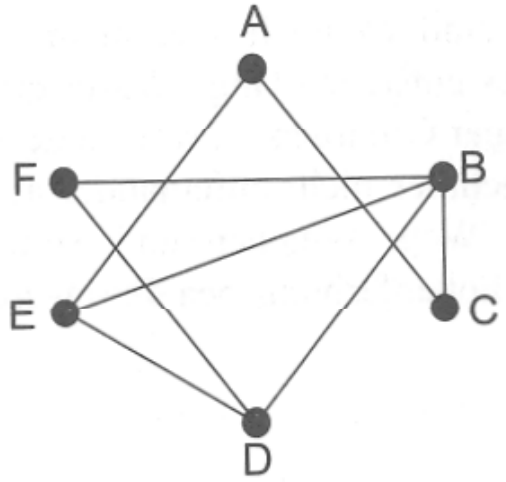
Konflikt-Graphen

Graphentheorie



Eine verkehrsreiche Einmündung

Konfliktgraphen.



Der Konfliktgraph der 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“

Osttirol mit „Venediger-Höhenweg“

Eine schroffe steinige Welt gangbar gemacht vom Alpenverein.

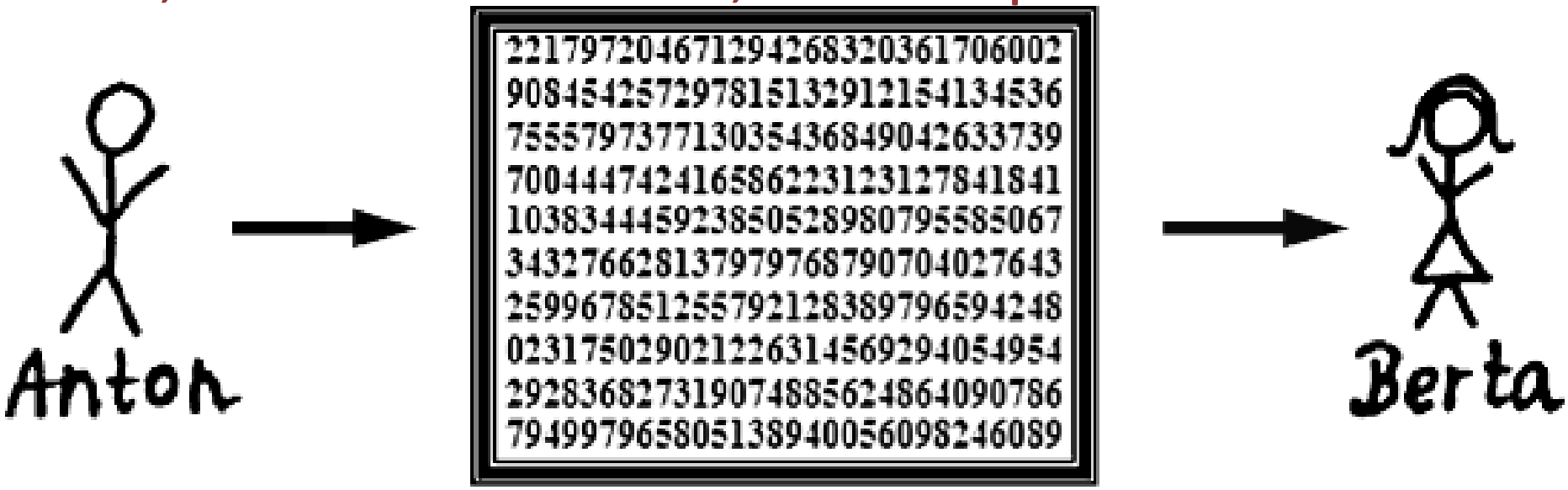
Als Alpenverein der Mathematik habe ich Sie hoffentlich einen gangbaren Weg geführt.

Vielen Dank für Ihre Aufmerksamkeit

Zugabe: Kryptografie

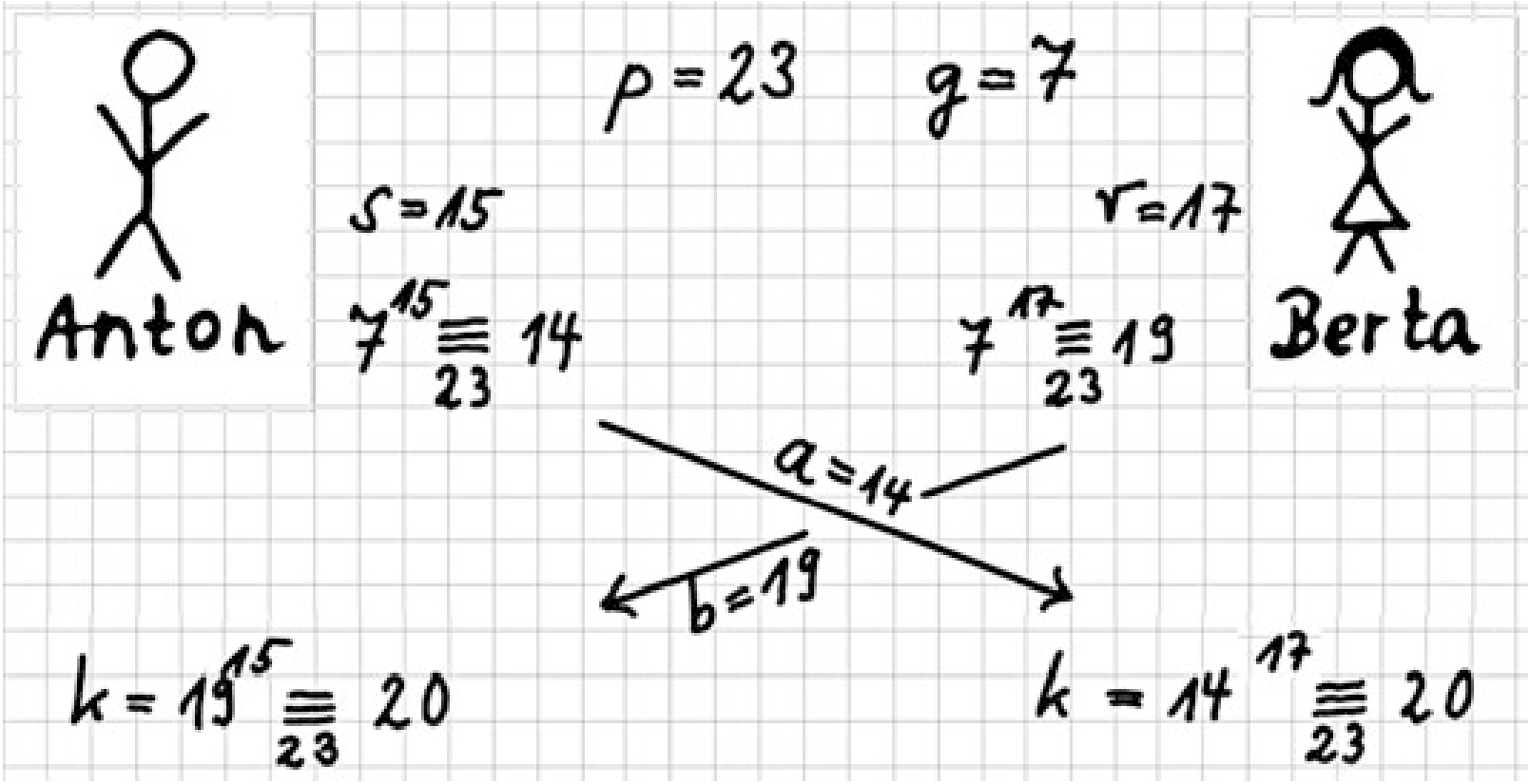
In der Ankündigung habe ich versprochen,
dass Sie etwas zu diesem Thema erfahren.

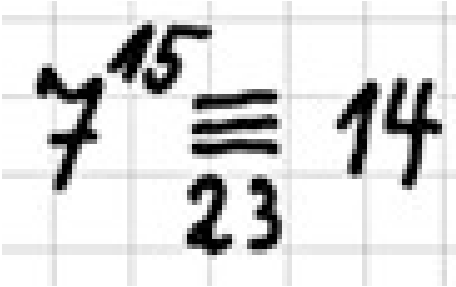
Nun, ich bin vorbereitet, das Versprechen zu halten.



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

Diffie-Hellman-Schlüssel

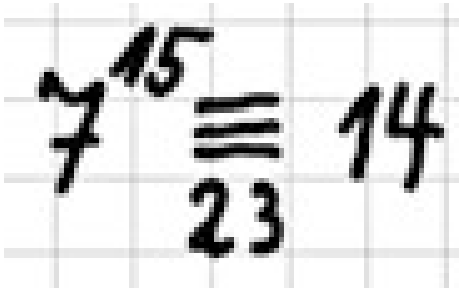




Lies: 7 hoch 15 modulo 23 ist 14

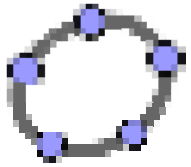
und was heißt das ?????????

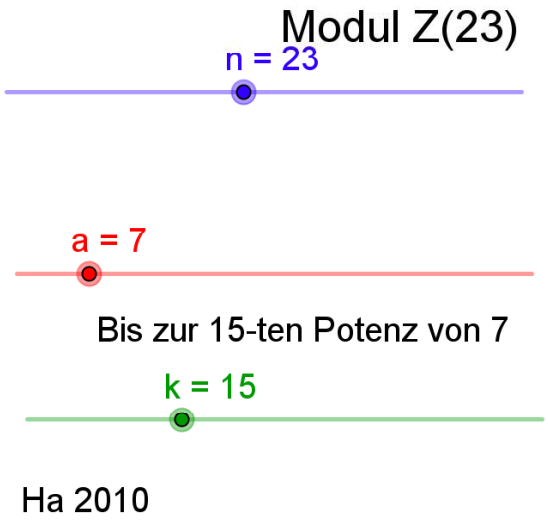
modulo-Potenzen

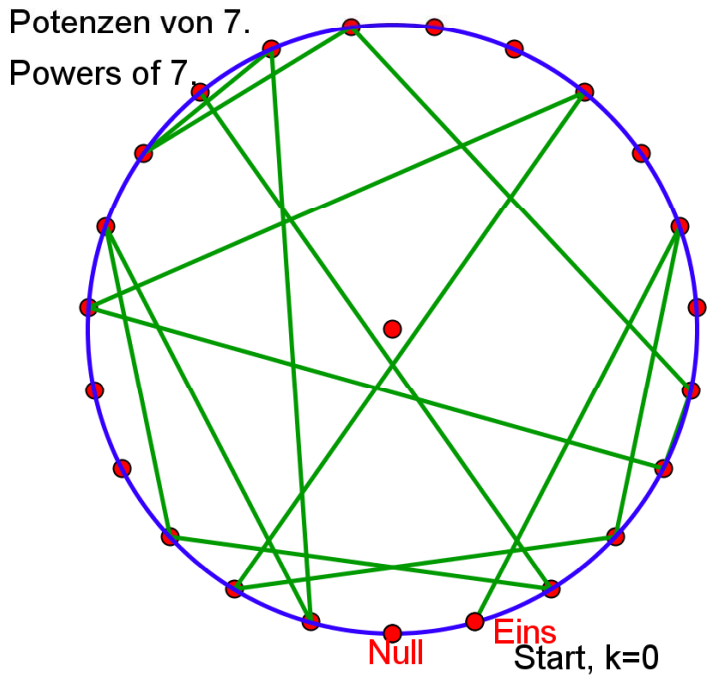


Lies: 7 hoch 15 modulo 23 ist 14

und was heißt das ?????????





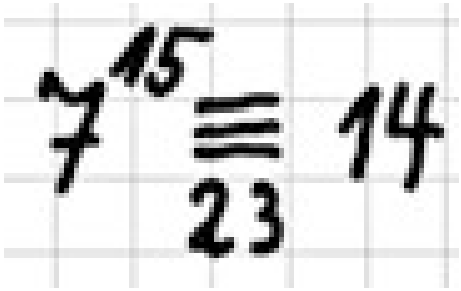


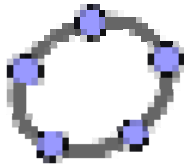
Potenzen von 7 in Z= {1, 7, 49, 343, 2401, 16807, 117649, 823543, 5764801, 40353607, 282475249, 19773267

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

11 Billiarden geht nicht mehr

modulo-Potenzen



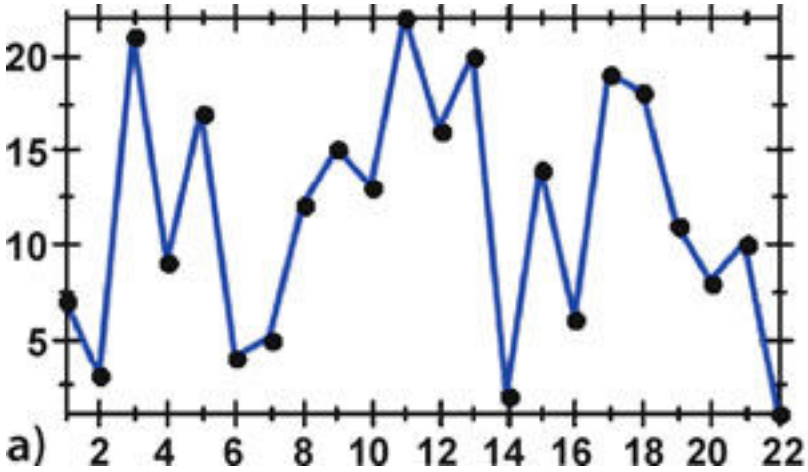


Das war zum Verstehen,
aber in Wahrheit sind die Zahlen riesig.

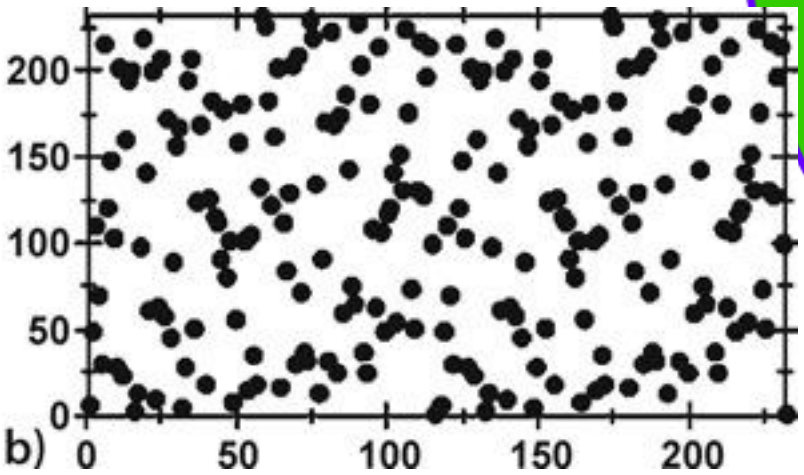
Primzahlen bei 10^{200}

Das Weltall enthält etwa 10^{90} Atome

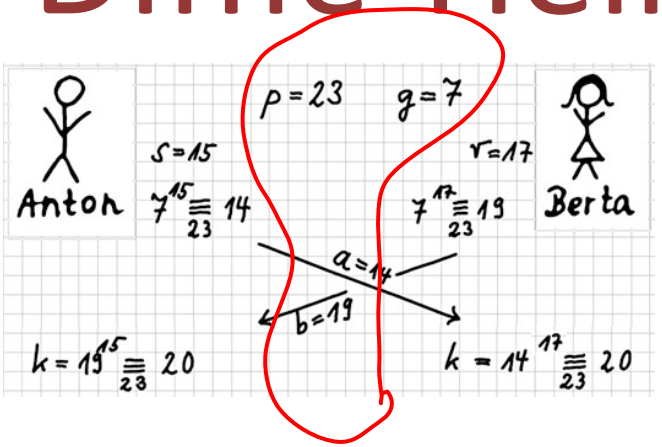
modulo 23



modulo 233



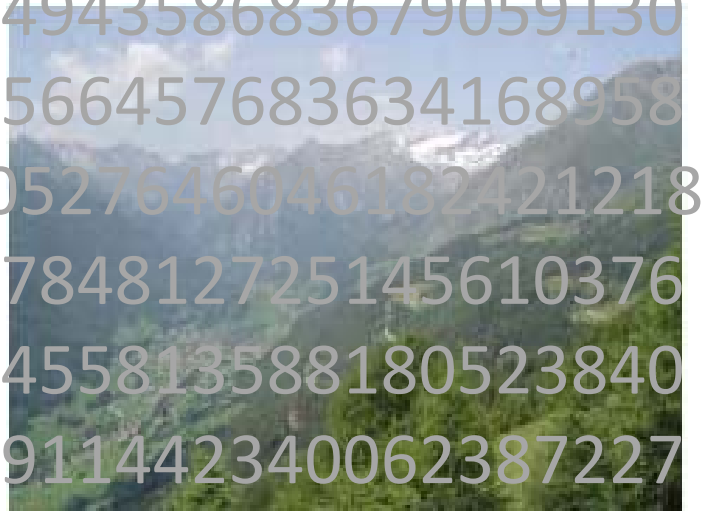
Diffie-Hellman-Schlüssel



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

Keine Chance!

Das waren jetzt die ganz hohen Gipfel!



Vielen Dank für Ihre Aufmerksamkeit

0438679462317222 Das sind p, g, a, kryptografisch echt.

Diffie-Hellmann-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
```