Leonhard Euler

und die moderne Mathematik

Hanspeter Kraft
Departement Mathematik und Informatik
Universität Basel

Volkshochschule beider Basel

Universität Basel

Eine Arbeit von Charles Hermite

Charles Hermite, französischer Mathematiker,
24. Dezember 1822 – 14. Januar 1901

Sur l'invariant du 18e ordre des formes du cinquième degré et sur le role qu'il joue dans la résolution de l'équation du cinquième degré, extrait de deux lettres de M. *Hermite* à l'éditeur.

Journal für Reine und Angewandte Mathematik
Band **59** (1861), 304-305

. . . J'ai entrepris en suivant la méthode de M. *Kronecker* de creuser un peu plus à fond la résolution de l'équation du 5e degré . . . . Chemin faisant j'ai eu à étudier l'invariant du 18e ordre des formes du cinquième degré qui joue un role fondamental dans la marche que j'ai suivie. Peut-être vous interessera-t-il de connaître comment il s'exprime au moyen des racines x_0, x_1, x_2, x_3, x_4 de la forme représentée par

$$f = a(x-x_0y)(x-x_1y)(x-x_2y)(x-x_3y)(x-x_4y).$$

Voici le résultat que j'ai obtenu. Soit pour abréger

$$(mn) = x_m - x_n,$$

on aura

$$\begin{aligned} I = a^{18}&\{(01)(04)(32)+(02)(03)(14)\}\{(01)(02)(43)+(03)(04)(12)\}\{(01)(03)(42)+(02)(04)(31)\}\\ &\times\{(12)(10)(43)+(13)(14)(20)\}\{(12)(13)(04)+(14)(10)(23)\}\{(12)(14)(03)+(13)(10)(42)\}\\ &\times\{(23)(21)(04)+(24)(20)(31)\}\{(23)(24)(10)+(20)(21)(34)\}\{(23)(20)(14)+(24)(21)(03)\}\\ &\times\{(34)(32)(10)+(30)(31)(42)\}\{(34)(30)(21)+(31)(32)(40)\}\{(34)(31)(20)+(30)(32)(14)\}\\ &\times\{(40)(43)(21)+(41)(42)(03)\}\{(40)(41)(32)+(42)(43)(01)\}\{(40)(42)(31)+(41)(43)(20)\} \end{aligned}$$

Les quinze facteurs ont été réunis trois à trois de manière à former cinq produits, symétriques chacuns par rapport à toutes les racines moins une. Le produit total est donc bien symétrique par rapport à toutes les racines, et l'on reconnait d'ailleurs immédiatement qu'il représente un invariant car il ne change pas quand on remplace les racines par leurs inverses et qu'on les augmente d'une même quantité . . . .

Désignons par X_0, X_1, X_2, X_3, X_4 les cinq produits de trois facteurs dont se compose l'expression de l'invariant I, de sorte que

$$X_0 = \{(01)(04)(32)+(02)(03)(14)\}\{(01)(03)(43)+(03)(04)(12)\}\{(01)(03)(42)+(02)(04)(31)\}$$

etc.

on peut écrire

$$I = a^{18}X_0X_1X_2X_3X_4$$

et X_k sera une fonction rationelle et entière de la seule racine x_k. Cela posé les quantités suivantes

$$\begin{aligned} z_0 &= a^6X_0(12)(13)(14)(23)(24)(34),\\ z_1 &= a^6X_1(23)(24)(20)(34)(30)(40),\\ z_2 &= a^6X_2(34)(30)(31)(40)(41)(01),\\ z_3 &= a^6X_3(40)(41)(42)(01)(02)(12),\\ z_4 &= a^6X_4(01)(02)(03)(12)(13)(23) \end{aligned}$$

seront elles mêmes sauf un facteur qui est la racine du discriminant, des fonctions rationelles semblables de x_0, x_1 etc., car on peut écrire par exemple en représentant le discriminant par Δ:

$$z_0 = a^3X_0\frac{\sqrt{\Delta}}{(01)(02)(03)(04)},$$

ce qui est évidemment une fonction rationnelle de x_0. Or l'équation du cinquième degré dont les racines seront ces quantités z_0, z_1 etc. aura pour coefficients des invariants, et sera de cette forme:

$$z^5+Lz^3+M\Delta z+I\sqrt{\Delta^3} = 0$$

L et M étant du 12e et du 16e ordre et I du 18e.

Exkurs: Lösen von Gleichungen

Quadratische Gleichungen (bereits im Altbabylonischen Reich bekannt)

$$x^2 + ax + b = 0: \qquad x_{1,2} = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

Idee: quadratische Ergänzung:

$$x^2 + ax + b = 0 \quad \Longleftrightarrow \quad \left(x + \frac{a}{2}\right)^2 + \left(b - \frac{a^2}{4}\right) = 0$$

Kubische Gleichungen (Formeln von Cardano 1545)

$$x^3 + ax^2 + bx + c = 0 \quad \Longrightarrow \quad x^3 + px + q = 0$$

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} - \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

Exkurs: Lösen von Gleichungen

Gleichungen 4. Grades: ebenfalls Formeln von Cardano (1545)

Gleichungen vom Grad > 4?

Évariste Galois (25. Okt. 1811 – 31. Mai 1832)

„Es gibt keine geschlossenen Formel für die Lösungen einer allgemeinen Gleichung vom Grad grösser oder gleich 5!“

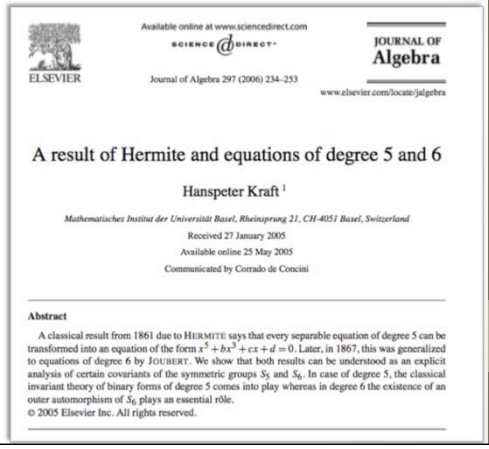
Moderne Forschung

Reduktion einer Gleichung n-ten Grades auf einfachere Form
(z.B. möglichst viele Koeffizienten = 0; Leopold Kronecker, Felix Klein, ...)

Joe Buhler & Zinovy Reichstein (Compositio Math. **106** (1997), 159-179): *„Es braucht mindestens n/2 verschiedene Koeffizienten."*

- Formel von **Hermite** (1861):
  $x^5 + a\,x^3 + b\,x + b = 0$
- Formel von **Joubert** (1867):
  $x^6 + a\,x^4 + b\,x^2 + c\,x + c = 0$

Erklärung?



Available online at www.sciencedirect.com
SCIENCE DIRECT
ELSEVIER
Journal of Algebra 297 (2006) 234–253
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

A result of Hermite and equations of degree 5 and 6

Hanspeter Kraft [1]

Mathematisches Institut der Universität Basel, Rheinsprung 21, CH-4051 Basel, Switzerland

Received 27 January 2005
Available online 25 May 2005
Communicated by Corrado de Concini

Abstract

A classical result from 1861 due to HERMITE says that every separable equation of degree 5 can be transformed into an equation of the form $x^5 + bx^3 + cx + d = 0$. Later, in 1867, this was generalized to equations of degree 6 by JOUBERT. We show that both results can be understood as an explicit analysis of certain covariants of the symmetric groups S_5 and S_6. In case of degree 5, the classical invariant theory of binary forms of degree 5 comes into play whereas in degree 6 the existence of an outer automorphism of S_6 plays an essential rôle.

Wer war Leonhard Euler?

- Ein wohlbekannter Basler?
- Ein weltberühmter Auslandschweizer?
- Der grösste Gelehrte seiner Zeit?
- Der führende Wissenschaftler des 18. Jahrhunderts?
- Einer der genialsten und produktivsten Mathematiker aller Zeiten?

oder

Der Mann mit der Nachthaube?

Der Mann auf der alten Zehnernote?

Der Mann auf der Briefmarke?

Der Auslandschweizer

1707 in Basel geboren (15. April)

1727 Basel → St. Petersburg

1741 St. Petersburg → Berlin

1766 Berlin → St. Petersburg

1783 in St. Petersburg verstorben (18. September)

„Er blieb seiner Vaterstadt immer eng verbunden, ist aber nie dahin zurückgekehrt.“

Der Gelehrte und Wissenschaftler

Fundamentale Beiträge zur Mathematik, Optik, Mechanik, Astronomie und Technik

Über 800 wissenschaftliche Arbeiten, etwa 3000 Briefe von und an Euler und rund 40'000 Manuskriptseiten

Philosophische und theologische Beiträge, sowie mehrere Schriften zur Musiktheorie

Der geniale Mathematiker

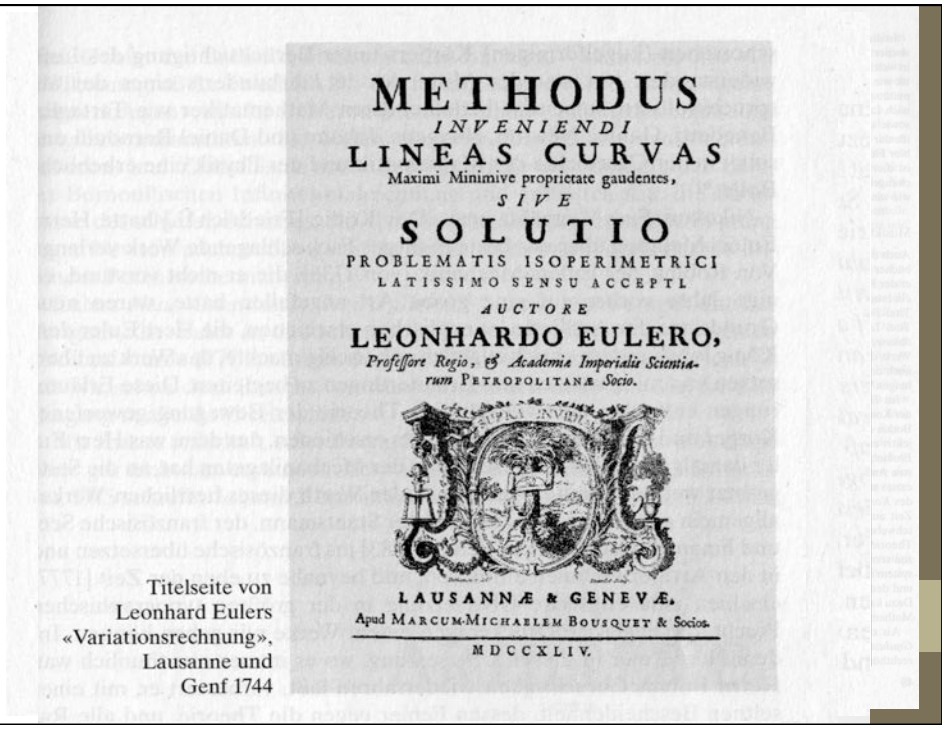
Viele originelle Ansätze und grundlegend neue Ideen

Enorme Breite und Tiefe in der Forschung

Grosse Ausstrahlung

Unvergleichliche Schaffenskraft

„Euler hat die Mathematik von Grund auf revolutioniert!"


METHODUS
INVENIENDI
LINEAS CURVAS
Maximi Minimive proprietate gaudentes,
SIVE
SOLUTIO
PROBLEMATIS ISOPERIMETRICI
LATISSIMO SENSU ACCEPTI
AUCTORE
LEONHARDO EULERO,
Professore Regio, & Academiæ Imperialis Scientiarum PETROPOLITANÆ Socio.
LAUSANNÆ & GENEVÆ,
Apud MARCUM-MICHAELEM BOUSQUET & Socios.
MDCCXLIV.

Titelseite von Leonhard Eulers «Variationsrechnung», Lausanne und Genf 1744

Wasserkunst in Sanssouci

Auftrag des Königs

Eulers Vorschläge und Berechnungen

Aber: die Rohre platzten!

Der Spott des Königs

«Je voulus faire un jet-d'eau en mon Jardin; le Ciclope Euler calcula l'éffort des roües, pour faire monter l'eau dans un bassin d'où elle devoit retomber par des canaux, afin de jaillir à Sans-Souci. Mon Moulin a été éxécuté géométriquement, et il n'a pu élever une goute d'eau à cinquante pas du Bassin. Vanité des Vanités; Vanité de la géométrie.»

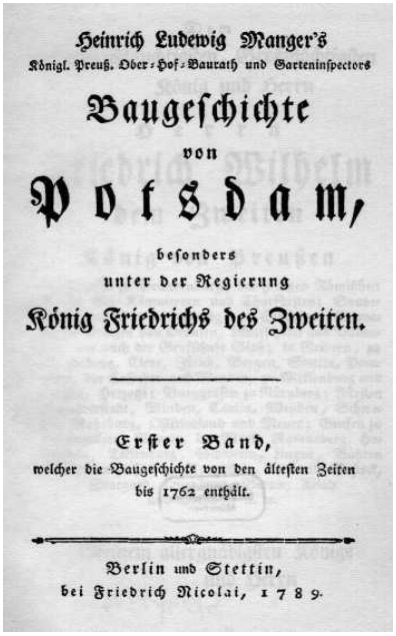
Friedrich II an Voltaire, 25. Januar 1778

„ ... zweitklassig als Physiker ...?"

„The physical universe was an occasion for mathematics to Euler, scarcely a thing of much interest in itself; and if the universe failed to fit his analysis it was the universe which was in error."
(E. T. Bell 1937)

„Der geniale Mathematiker Euler war zweitklassig als Physiker ..."
(A. Hermann 1991)

„When Euler applied his equations to design a fountain for Frederick the Great of Prussia, it failed to work ... Unfortunately, he omitted the effects of friction, with embarrassing practical consequences."
(S. Perkovitz 1999)

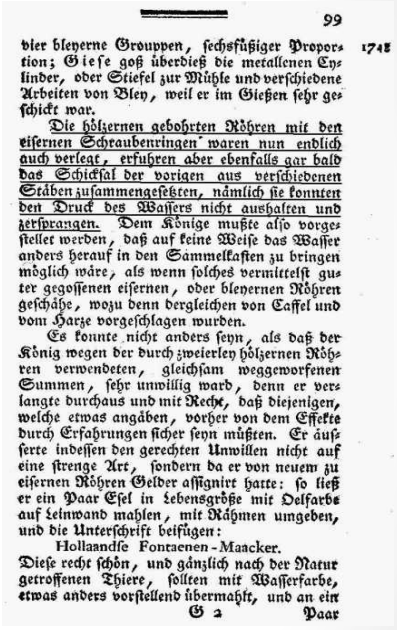


Heinrich Ludewig Manger's
Königl. Preuß. Ober-Hof-Baurath und Garteninspectors

Baugeschichte
von
Potsdam,
besonders
unter der Regierung
König Friedrichs des Zweiten.

Erster Band,
welcher die Baugeschichte von den ältesten Zeiten
bis 1762 enthält.

Berlin und Stettin,
bei Friedrich Nicolai, 1789.



99

vier bleyerne Grouppen, sechsfüßiger Proportion; Diese goß überdieß die metallenen Cylinder, oder Stiefel zur Mühle und verschiedene Arbeiten von Bley, weil er im Gießen sehr geschickt war. 1748

Die hölzernen gebohrten Röhren mit den eisernen Schraubenringen waren nun endlich auch verlegt, erfuhren aber ebenfalls gar bald das Schicksal der vorigen aus verschiedenen Stäben zusammengesetzten, nämlich sie konnten den Druck des Wassers nicht aushalten und zersprangen. Dem Könige mußte also vorgestellet werden, daß auf keine Weise das Wasser anders herauf in den Sammelkasten zu bringen möglich wäre, als wenn solches vermittelst guter gegossenen eisernen, oder bleyernen Röhren geschähe, wozu denn dergleichen von Cassel und vom Harze vorgeschlagen wurden.

Es konnte nicht anders seyn, als daß der König wegen der durch zweierley hölzernen Röhren verwendeten, gleichsam weggeworfenen Summen, sehr unwillig ward, denn er verlangte durchaus und mit Recht, daß diejenigen, welche etwas angäben, vorher von dem Effekte durch Erfahrungen sicher seyn müßten. Er äusserte indessen den gerechten Unwillen nicht auf eine strenge Art, sondern da er von neuem zu eisernen Röhren Gelder assignirt hatte: so ließ er ein Paar Esel in Lebensgröße mit Oelfarbe auf Leinwand mahlen, mit Rähmen umgeben, und die Unterschrift beifügen:

Hollaandse Fontaenen-Maacker.

Diese recht schön, und gänzlich nach der Natur getroffenen Thiere, sollten mit Wasserfarbe, etwas anders vorstellend übermahlt, und an ein

G 2 Paar

Eulers Auftrag

„Je prend la liberté de vous addresser mes recherches sur la Machine Hydraulique de Sans-Soucy ... je crains fort qu'il s'en faudra beaucoup qu'elle monte à la hauteur que Le Roy souhaite ...“

(Euler an Maupertuis, 21. September 1749)

„Comme Sa Majesté le Roy de Prusse, Notre très gracieux Souverain, a reçu les calculs que le professeur Euler Lui a adressé au sujet de la Machine de Sans-Soucy et qu'Elle en est fort contente, Sa Majesté veut bien lui témoigner tout le gré ...“

(Friedrich II. an Euler, 27. September 1749)

Eulers Warnungen!

„Car sur le pied qu'elles se trouvent actuellement, il est bien certain, qu'on n'éleveroit jamais une goutte d'eau jusqu'au réservoir, et toute la force ne seroit employée qu'à la destruction de la machine et des tuyaux.“

(Euler an Friedrich II, 17. Oktober 1749)

„La véritable cause de ce fâcheux accident consistoit uniquement en ce que la capacité des pompes étoit trop grande, et à moins qu'on ne la diminue très considérablement, ou en diminuant leur diamètre ou leur hauteur, ou le nombre des jeux qui repond à un tour de moulin, la machine ne sera pas en état de fournir une seule goûte d'eau dans le réservoir.“

(Euler an Maupertuis, 21. Oktober 1749)

Fazit

Eulers Analyse des Sanssouci-Problems war korrekt. Sie begründete die moderne Hydraulik.

Die daraus abgeleiteten praktischen Regeln wurden ignoriert.

Das Wasserkunst-Projekt in Sanssouci scheiterte, weil der König unfähige Praktiker pfuschen liess und vor den hohen Ausgaben zurückschreckte.

Eulers Hydrodynamik beruhte auf jahrelanger Erfahrung mit praktischen Problem wie dem in Sanssouci.

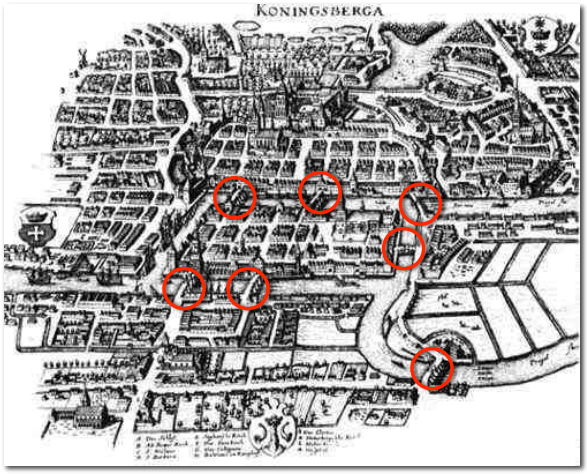
Eulers Mathematik
Drei Beispiele

Das Königsberger Brückenproblem

Die Eulersche Polyederformel $e - k + f = 2$

Der Eulersche Satz $x^{\varphi(n)} = 1 \mod n$

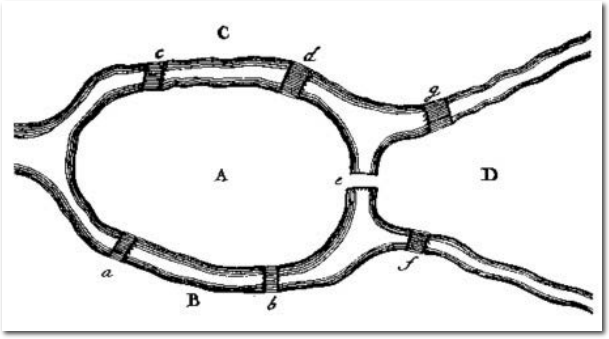
Das Königsberger Brückenproblem



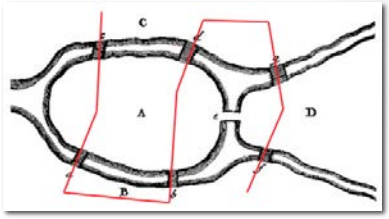
Königsberg (Kaliningrad) am Pregel, mit den 7 Brücken

Frage

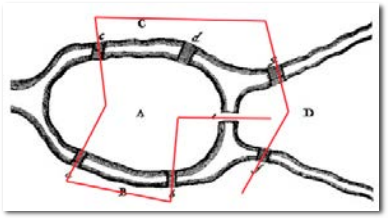
Gibt es einen Spaziergang durch Königsberg, bei dem man jede der 7 Brücken genau einmal überschreitet?



Erster Versuch:



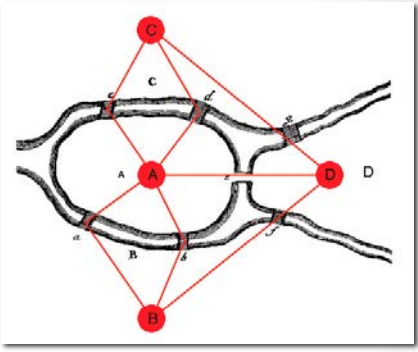
Zweiter Versuch:



„Es scheint nicht zu gehen! Aber warum nicht und wie sieht man das ein?“

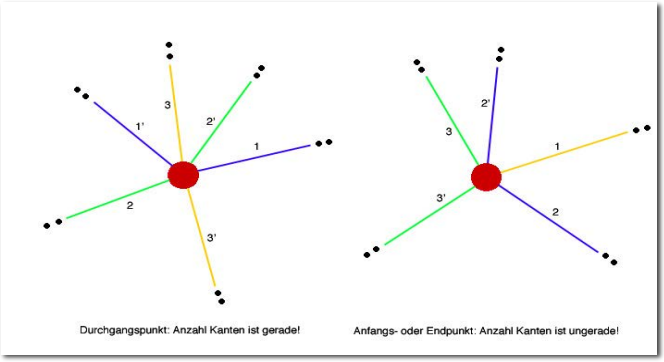
Graphentheorie

Definition
Ein *Graph* besteht aus Punkten (= Ecken), die durch Strecken (= Kanten) verbunden sind.



Allgemeines Problem
Gegeben ein beliebiger Graph. *Gibt es einen Weg durch diesen Graphen, der jede Kante genau einmal benutzt?*

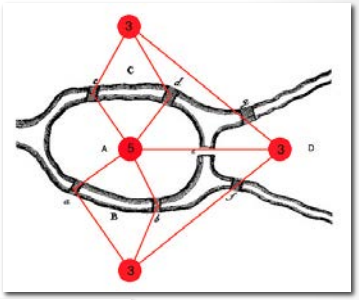
Was passiert bei einem solchen Spaziergang?



Notwendige Bedingung („Valenzbedinung“): *Die Anzahl der von einer Ecke ausgehenden Kanten ist gerade, eventuell mit genau zwei Ausnahmen.*

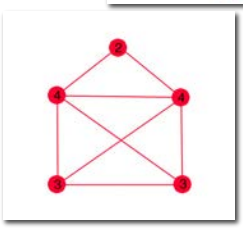
Königsberger Brückengraph

Erfüllt die notwendige Valenz-bedingung nicht! ☛ Es gibt daher keinen solchen Spaziergang!



Satz von Euler: *Valenzbedingung ist auch hinreichend, um einen solchen Spaziergang zu finden!*

Beispiel: Das Nikolaushaus



136] AD GEOMETRIAM SITUS PERTINENTIS 7

15. Sint duae insulae *A* et *B* aqua circumdatae, qua cum aqua communicent quatuor fluvii, quemadmodum figura (Fig. 3) repraesentat. Traiecto porro sint super aquam insulas circumdantem et fluvios quindecim pontes *a*, *b*, *c*, *d* etc. et quaeritur, num quis cursum ita instituere queat, ut per

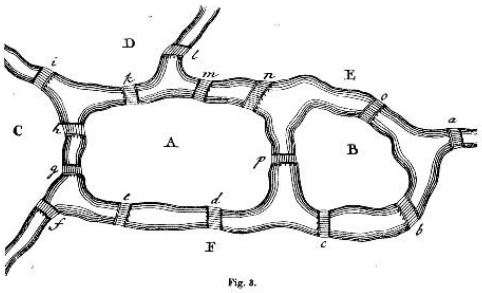
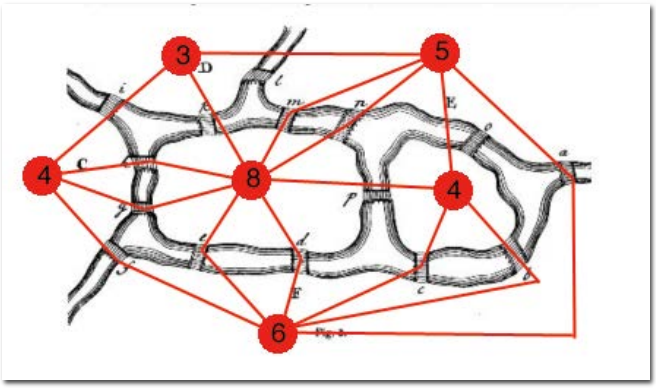


Fig. 3.

omnes pontes transeat, per nullum autem plus quam semel. Designo ergo primum omnes regiones, quae aqua a se invicem sunt separatae, litteris *A*, *B*, *C*, *D*, *E*, *F*, cuiusmodi ergo sunt sex regiones. Dein numerum pontium 15 unitate augeo et summam 16 sequenti operationi praefigo.

		16
*A**,	8	4
*B**,	4	2
*C**,	4	2
D,	3	2
E,	5	3
*F**,	6	3
		16



Die Eulerschen Valenzbedingungen sind erfüllt.
Es gibt also einen solchen Spaziergang!

Anwendungen der Graphentheorie

- Transportprobleme
- Navigationssysteme
- Ökonomie (optimale Verteilungen)
- Bau von Mikrochips
- usw.

Zusammenfassung

- Ausgangspunkt: ein praktisches Problem
- Ansatz: Abstraktion (Reduktion auf das Wesentliche)
  ☛ Graphen
- Verallgemeinerung ☛ Lösung
- Weiterentwicklung ☛ Graphentheorie

Neue, unvorhergesehene und überraschende Anwendungen!

Die Polyederformel: $e - k + f = 2$

Polyeder oder Vielflächner: konvexer Körper, der durch Vielecke begrenzt ist.

Formel: e = Anzahl Ecken, k = Anzahl Kanten, f = Anzahl Flächen

356 DEMONSTRATIO

SCHOLION.

17. Quanquam alterum Theorema ita ab hoc pendet, vt cum hoc fuerit demonstratum, simul illius veritas sit euicta, tamen ex problemate praemisso etiam alterius Theorematis demonstratio conflci potest sequenti modo.

PROPOSITIO IV. THEOREMA.

18. *In omni solido hedris planis incluso numerus hedrarum vna cum numero angulorum solidorum, binario excedit numerum acierum.*

DEMONSTRATIO.

Sit in solido quocunque proposito:
numerus angulorum solidorum = S
numerus hedrarum ~ - - = H
numerus acierum - - - = A
atque ante vidimus, si resectione vnius anguli solidi numerus S vnitate minuatur, vt fit S − 1, tum differentiam inter numerum acierum et numerum hedrarum futuram esse = A − H − 1. Continuata ergo hac mutilatione,

si numerus angulorum solidorum sit,	Excessus numeri acierum super numerum hedrarum erit:
S	A − H
S − 1	A − H − 1
S − 2	A − H − 2
S − 3	A − H − 3
:	:
:	:
S − n	A − H − n

Quando

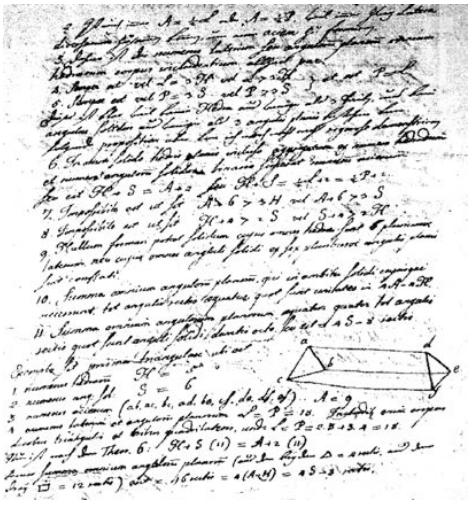
PROPRIETATVM SOLIDORVM. 157

Quando ergo hoc modo ad pyramidem triangularem deuenietur, in qua numerus angulorum solidorum est = 4, numerus hedrarum = 4, et numerus acierum = 6, ita vt excessus numeri acierum supra numerum hedrarum futurus sit = 2; euidens est, si fiat S − n = 4, fore A − H − n = 2. Inde ergo est n = S − 4, hinc vero n = A − H − 2; sicque habebitur S − 4 = A − H − 2, seu H + S = A + 2; vnde constat, in omni solido hedris planis incluso numerum hedrarum H vna cum numero angulorum solidorum S binario superare numerum acierum A. Q. E. D.

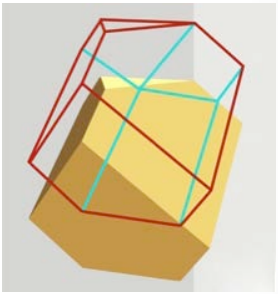
$H + S = A + 2$

S = numerus angulorum solidorum
H = numerus hedrarum
A = numerus acierum

Unregelmässige Polyeder



Brief an Christian Goldbach (1750):
$H + S = A + 2$



1 Dreieck, 5 Vierecke, 3 Fünfecke
$e = 12, k = 19, f = 9$

Der Fussball

Klassischer Fussball:
Pentakisdodekaeder mit
12 Fünfecken und
20 Sechsecken

e = 60 = (60 + 120)/3
k = 90 = (60 + 120)/2
f = 32 = 12 + 20

☛ *e - k + f = 2*

Was ist daran so erstaunlich?

- Sehr einfache Aussage, leicht nachprüfbar
- Universelle Gültigkeit
- Geniale Intuition
- Ungeahnte Auswirkungen:
  Basis der „algebraischen Topologie"

Der Eulersche Satz: $x^{\varphi(n)} = 1 \bmod n$

- Elementare Zahlentheorie, geht auf **Fermat** zurück:
  $x^p = x \bmod p$
- Anspruchsvolle Spielerei?
- **Fermatsche Vermutung**:
  $x^n + y^n = z^n$
  ist unlösbar in ganzen Zahlen x,y,z für n>2.
  - ☛ Entwicklung der modernen Zahlentheorie
- Nützlichkeit? Anwendungen?

Daniel Bernoulli an Nicolaus Fuss

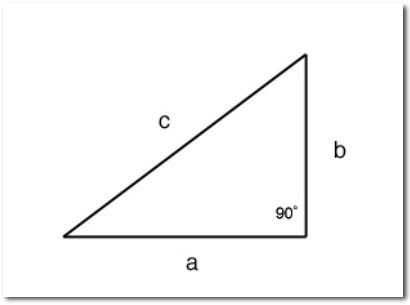
(Brief vom 18. März 1776)

« Ce que vous me dites ... est sans doute infiniment sublime; je veux parler du beau théorème de M. Euler sur les nombres premiers et de sa nouvelle méthode pour examiner tel nombre qu'on propose, quelque grand qu'il puisse être, s'il est premier, ou non. Ce que vous vous êtes donné la peine de me dire sur cette matière m'a paru fort subtil et digne de notre grand maître. Mais ne trouvez vous pas que c'est presque faire trop d'honneur aux nombres premiers que d'y répandre tant de richesses, et ne doit-on aucun égard au goût raffiné de notre siècle? Je ne laisse pas de rendre justice à tout ce qui sort de votre plume et d'admirer vos grandes ressources pour surmonter les difficultés les plus épineuses, mais cette admiration se redouble quand le sujet peut mener à des connoissances utiles. »

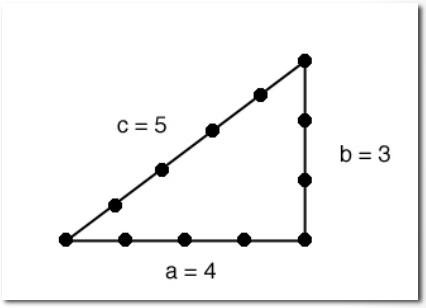
Daniel Bernoulli
8. Februar 1700 – 17. März 1782

Pythagoras!

$a^2 + b^2 = c^2$



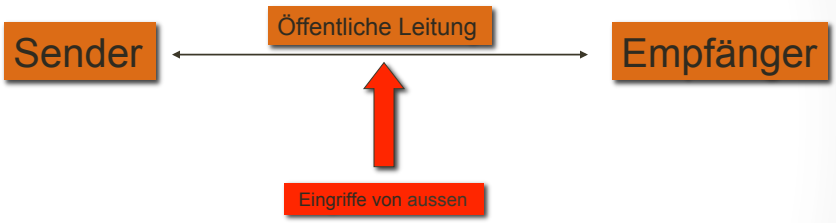
Ganzzahlige Lösungen?



$4^2 + 3^2 = 5^2$

☛ *Landvermessung im alten Ägypten!*

Exkurs:
Internet und öffentliche Netzwerke



Man muss davon ausgehen, dass die Leitung öffentlich ist und dass alle verwendeten Geräte und Verfahren bekannt sind.

Probleme von „öffentlichen" Netzwerken

Vertraulichkeit und Sicherheit

- *Geheimhaltung (Abhören)*
- *Authentifizierung*
- *Eindringen („Hacken")*

Schutzmassnahmen

Klassisch:
Kuriere, eingeschriebene Sendungen, Unterschrift, Ausweis, usw.

Digital:
- Geheimhaltung durch Verschlüsselung (Chiffrierung)
- Authentifizierung durch digitale Unterschrift

Für die digitalen Methoden braucht es **Passwörter**!

- Persönliche Passwörter
- Streichlisten (einmaliger Gebrauch)
- Kartenleser
- 3-D Secure (Smartphone mit Transakt-App) usw.

Digitale Verschlüsselung (Chiffrierung)

Es gibt absolut sichere Chiffrierverfahren!

- Gemeinsamer geheimer „Schlüssel" für Sender und Empfänger
- Regelmässige Änderung des Schlüssels

Problem:
Schlüsselverwaltung und Schlüsselaustausch (viele Partner!)

„Öffentliche Geheimhaltung"

Public Key Cryptography

Öffentlicher Schlüsseltausch (W. Diffie und M.E. Hellman, Stanford University 1976):

Austausch eines geheimen Schlüssels über eine öffentliche Leitung

RSA-Kryptosystem (R. Rivest, A. Shamir, L. Adleman 1977):

Chiffrierung mit Hilfe eines öffentlichen Schlüssels, Dechiffrierung nur mit geheimem Schlüssel möglich

Beide Systeme verwenden Methoden der elementaren Zahlentheorie und sogenannte „Einweg-Funktionen".

- Diffie-Hellman: Potenzieren versus diskreter Logarithmus
- RSA: Produkt grosser Primzahlen + Euler-Formel

Anwendungen

Diffie-Hellman Key Exchange

- On-line Zahlungen
- E-Banking
- E-Commerce
- E-Voting (elektronische Abstimmungen)

RSA-Kryptosystem

- E-Mail (PGP-Algorithmus)
- Übermittlung von Passwörtern
- Digitale Unterschrift
- Signieren von elektronischen Dokumenten

Zusammenfassung

- Kryptographie und Kodierungstheorie: Basis für den sicheren Datenaustausch
- Beruhen auf Methoden der elementaren Zahlentheorie
- Eulersche Formel spielt eine wichtige Rolle (z.B. beim RSA-Kryptosystem)

Eine Entdeckung der elementaren Zahlentheorie findet 250 Jahre später eine erstaunliche Anwendung, die heute im täglichen Leben eine zentrale Rolle spielt!

Bemerkungen

- Diffie und Hellman waren nicht die ersten!
  (Britischer Geheimdienst: J. Ellis, C. Cocks, M. Williamson kannten die Methode schon 1970!)
- Quantum-Computing (viel schnellere Algorithmen!)

Die Testfrage

Was würden Sie ohne Euler und die Mathematik tun?

Barzahlen!

Vielen Dank für Ihre Aufmerksamkeit

BERNOULLI EULER ZENTRUM

http://www.bez.unibas.ch
http://www.beg.unibas.ch

BERNOULLI EULER GESELLSCHAFT