HAL open science

Quelques épisodes dans l'histoire de l'algèbre effective

Catherine Goldstein

To cite this version:

Catherine Goldstein. Quelques épisodes dans l'histoire de l'algèbre effective. École thématique. Journées nationales de calcul formel, Luminy, France. 2019. hal-04117560

HAL Id: hal-04117560

https://hal.science/hal-04117560

Submitted on 5 Jun 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Quelques épisodes dans l'histoire de l'algèbre effective

CATHERINE GOLDSTEIN

INSTITUT DE MATHEMATIQUES
DE JUSSIEU-PARIS RIVE GAUCHE
catherine.goldstein@imj-prg.fr

Quelques épisodes (qui devraient être intégrés) dans l'histoire de l'algèbre effective

CATHERINE GOLDSTEIN

INSTITUT DE MATHEMATIQUES
DE JUSSIEU-PARIS RIVE GAUCHE
catherine.goldstein@imj-prg.fr

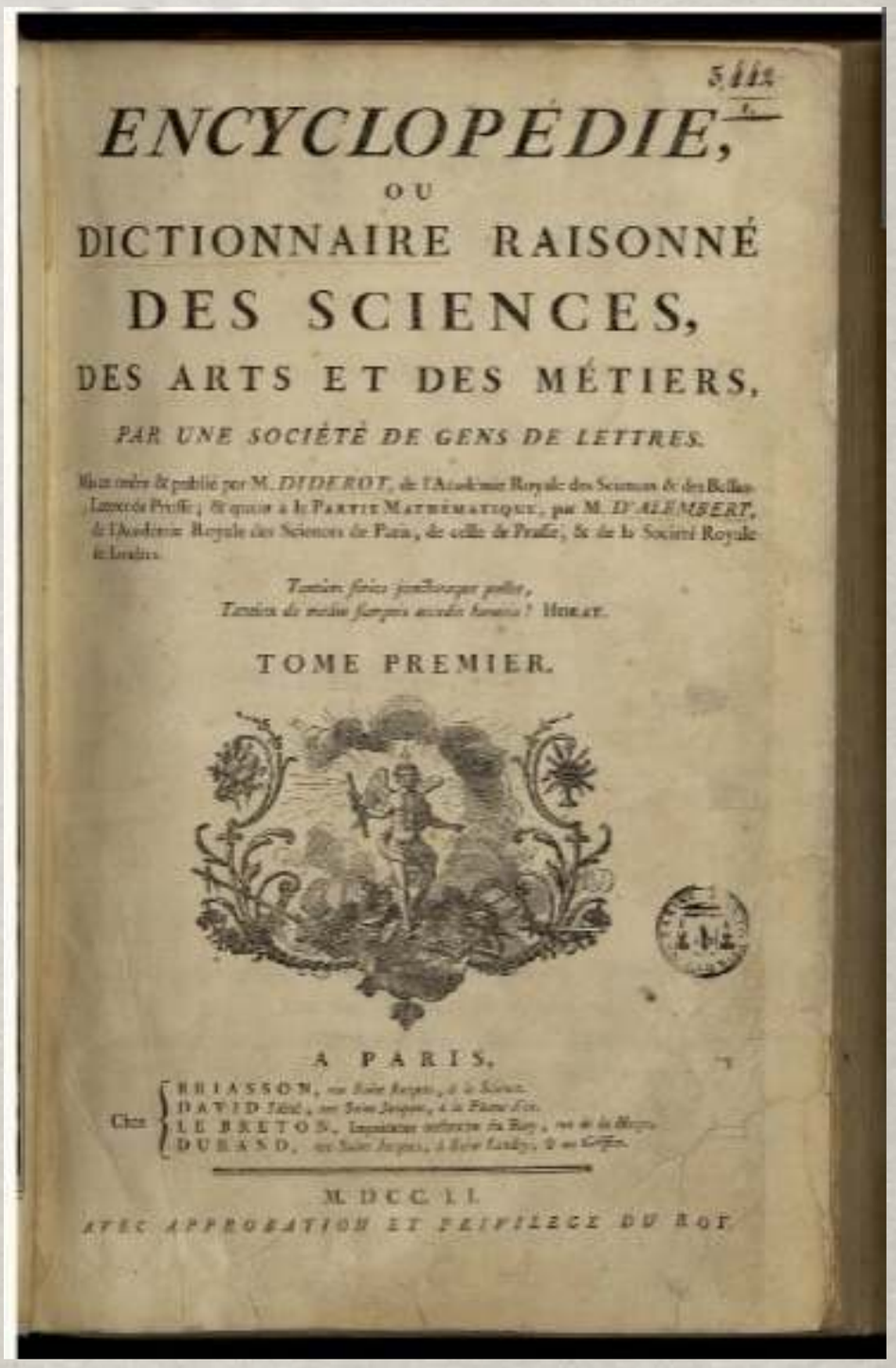
Quelques problèmes

- qu’est-ce qui compte comme “effectif” ?
- qu’est-ce qui compte comme “algèbre” ?
- qu’est-ce qui compte comme “histoire” ?

ALGEBRE, s. f. : c'est la méthode de faire en général le calcul de toutes sortes de quantités, en les représentant par des signes très-universels. On a choisi pour ces signes les lettres de l'alphabet, comme étant d'un usage plus facile & plus commode qu'aucune autre sorte de signes.

ALGORITHME, s. m. terme arabe, employé par quelques Auteurs, & singulierement par les Espagnols, pour signifier la pratique de l'Algebre. […] L'algorithme, selon la force du mot, signifie proprement l'Art de supputer avec justesse & facilité.

[O : d'Alembert, *Encyclopédie*]


ENCYCLOPÉDIE,
OU
DICTIONNAIRE RAISONNÉ
DES SCIENCES,
DES ARTS ET DES MÉTIERS,
PAR UNE SOCIÉTÉ DE GENS DE LETTRES.
TOME PREMIER.
A PARIS,
M. DCC. LI.
AVEC APPROBATION ET PRIVILEGE DU ROI.

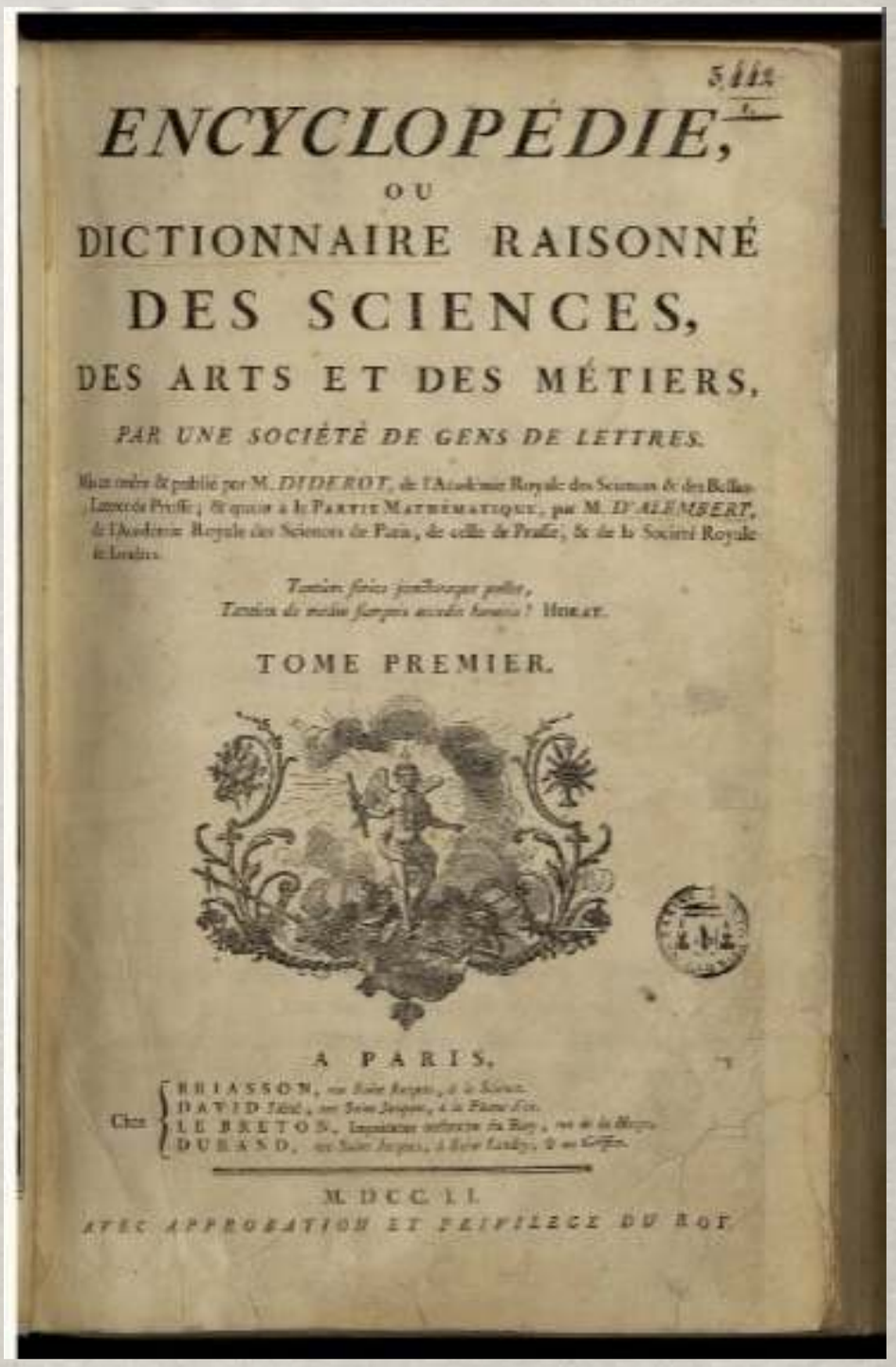
http://enccre.academie-sciences.fr/

Construction, s. f. Ce mot exprime, en Géométrie, les opérations qu'il faut faire pour exécuter la solution d'un problème. La construction d'une équation, est la méthode d'en trouver les racines par des opérations faites avec la regle & le compas, ou en général par la description de quelque courbe.

[O : d'Alembert, *Encyclopédie*]

EFFECTIF, adj. qui est réel & positif. Dans le Commerce, un payement effectif est celui qui se fait véritablement & en deniers comptans, ou effets équivalens.

[G : Edme François Mallet, *Encyclopédie*]



ENCYCLOPEDIE,

OU

DICTIONNAIRE RAISONNÉ

DES SCIENCES,

DES ARTS ET DES MÉTIERS,

PAR UNE SOCIÉTÉ DE GENS DE LETTRES.

TOME PREMIER.

A PARIS,

M. DCC. LI.

AVEC APPROBATION ET PRIVILEGE DU ROI.

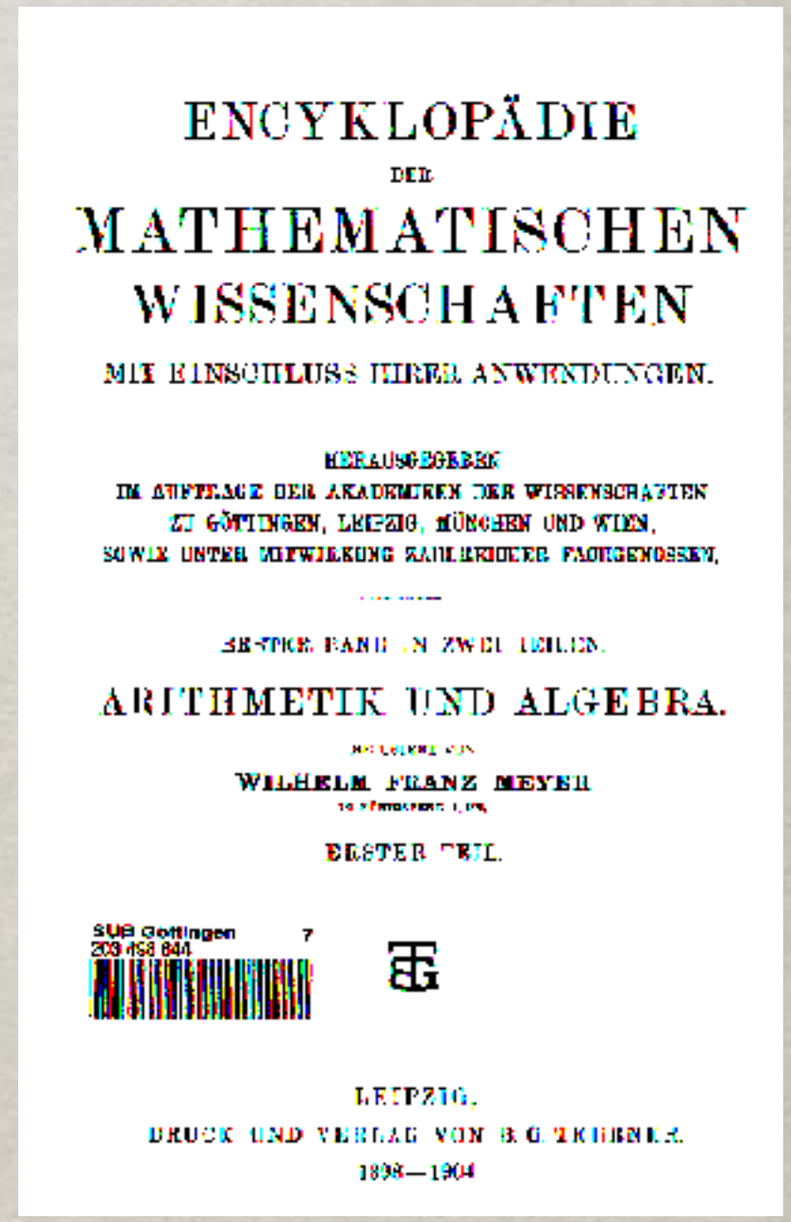
http://enccre.academie-sciences.fr/

Au cours du 19e siècle

- déterminants et invariants
- formes linéaires, quadratiques, bilinéaires, etc
- matrices, groupes
- anneaux, modules, corps
- nombres complexes et réels, etc…

L'algèbre dans l'Encyclopédie de Meyer, Klein, etc

- Arithmétique
  - Fondements
  - Combinatoire (coefficients binomiaux, déterminants, matrices)
  - Nombres irrationnels et suites (limites, fractions continues)
  - Grandeurs complexes
  - Théorie des ensembles
  - Groupes finis
- Algèbre
  - Fonctions rationnelles d'une variable
  - Fonctions rationnelles de plusieurs variables
  - Théorie arithmétique des grandeurs algébriques
  - Invariants
  - Séparation et approximation des racines
  - Fonctions rationnelles des racines
  - Théorie de Galois


ENCYKLOPÄDIE
DER
MATHEMATISCHEN
WISSENSCHAFTEN
MIT EINSCHLUSS IHRER ANWENDUNGEN.

HERAUSGEGEBEN
IM AUFTRAGE DER AKADEMIEN DER WISSENSCHAFTEN
ZU GÖTTINGEN, LEIPZIG, MÜNCHEN UND WIEN,
SOWIE UNTER MITWIRKUNG ZAHLREICHER FACHGENOSSEN.

SECHSTER BAND IN ZWEI TEILEN.

ARITHMETIK UND ALGEBRA.

WILHELM FRANZ MEYER

ERSTER TEIL.

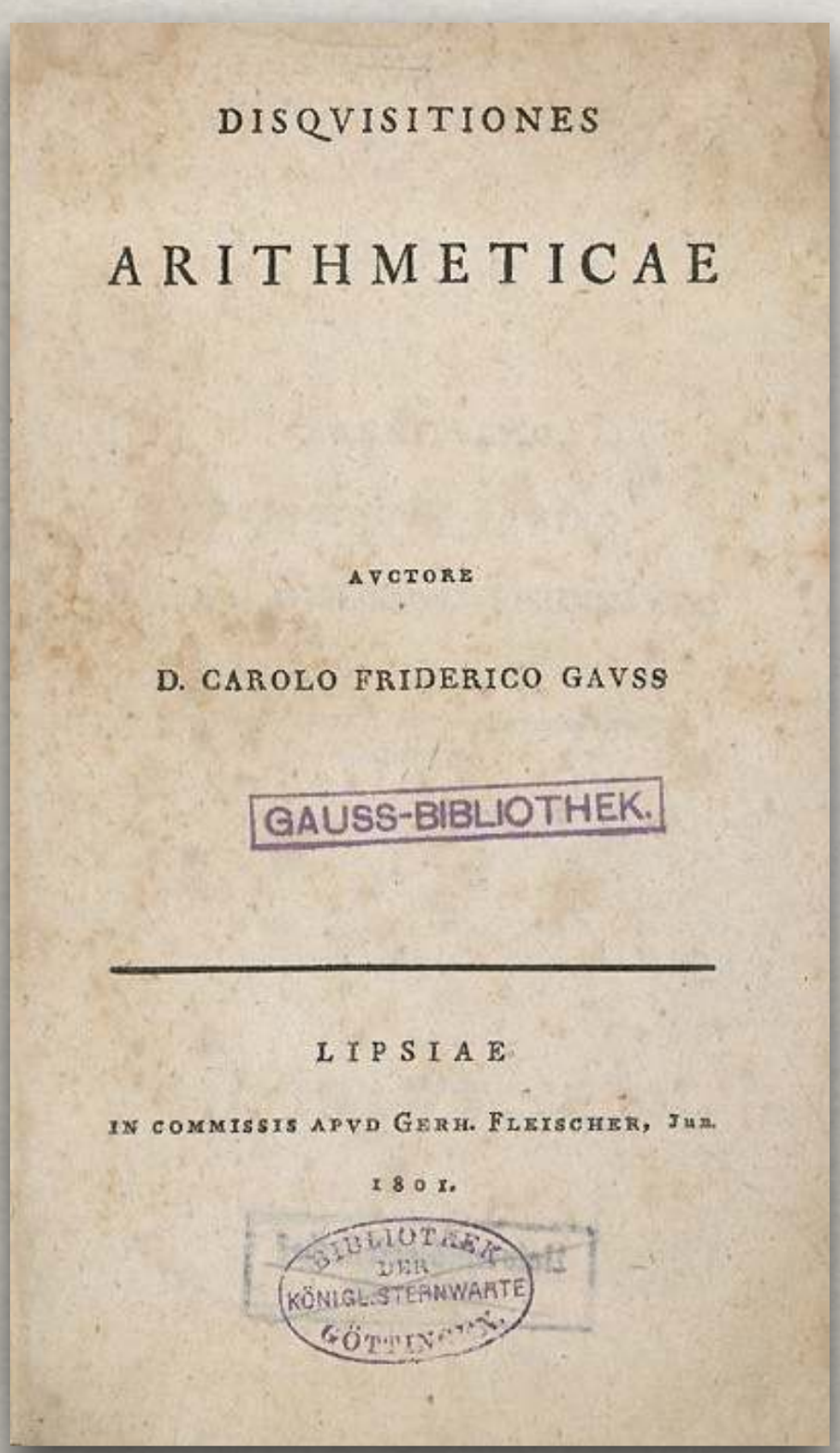
SUB Göttingen 7
203 458 844

LEIPZIG.
DRUCK UND VERLAG VON B. G. TEUBNER.
1898—1904

Quelques miettes historiques autour de l'effectivité et de l'algèbre

CATHERINE GOLDSTEIN

INSTITUT DE MATHEMATIQUES
DE JUSSIEU-PARIS RIVE GAUCHE
catherine.goldstein@imj-prg.fr



DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

GAUSS-BIBLIOTHEK.

LIPSIAE

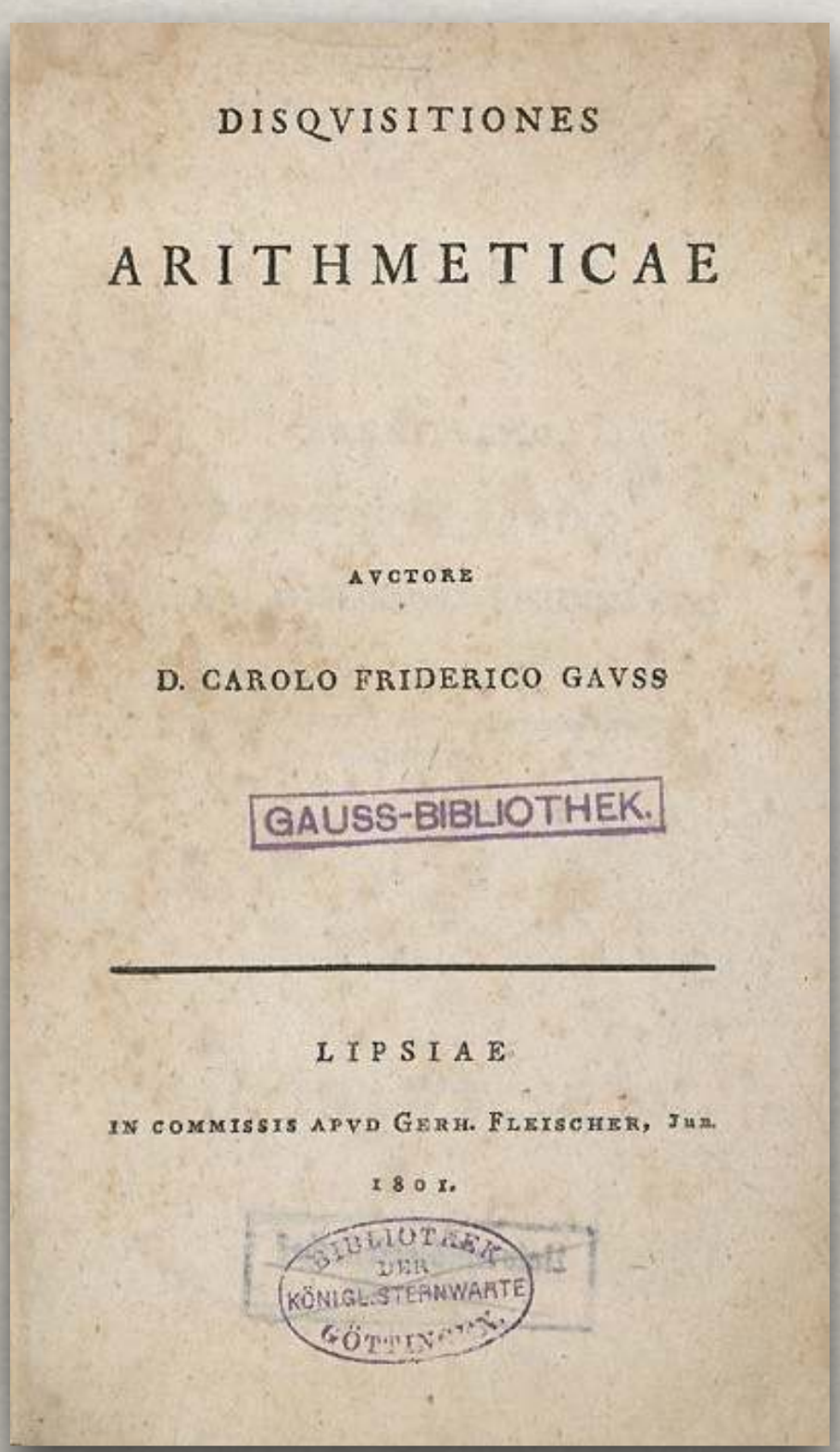
IN COMMISSIS APVD GERH. FLEISCHER, JUN.

1801.

BIBLIOTHEK DER KÖNIGL. STERNWARTE GÖTTINGEN

Carl Friedrich Gauss (1777-1855)

portrait par J.C.A. Schwartz, 1803



DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

GAUSS-BIBLIOTHEK.

LIPSIAE

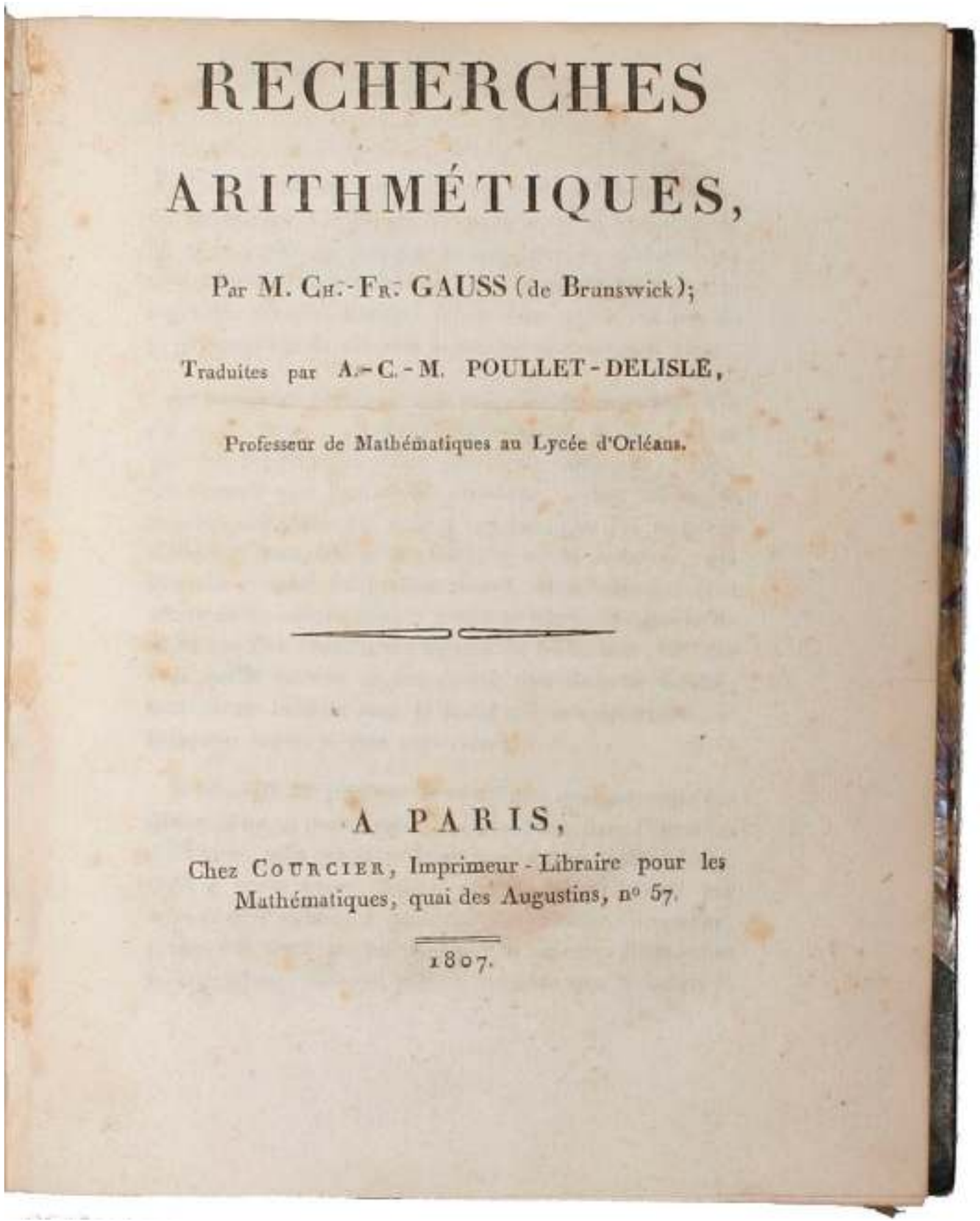
IN COMMISSIS APVD GERH. FLEISCHER, JUN.

1801.

BIBLIOTHEK DER KÖNIGL. STERNWARTE GÖTTINGEN.

Il ne peut y avoir aucun doute sur l'importance des *Disquisitiones Arithmeticae de Gauss* pour le développement des mathématiques. C'est un ouvrage qui a en mathématiques à peu près la même position que la *Critique de la raison pure* de Kant en philosophie.

Carl Itzigsohn à Julius Springer, 23 mars 1885



RECHERCHES ARITHMÉTIQUES,

Par M. Ch.-Fr. GAUSS (de Brunswick);

Traduites par A.-C.-M. POULLET-DELISLE,

Professeur de Mathématiques au Lycée d'Orléans.

A PARIS,

Chez COURCIER, Imprimeur-Libraire pour les Mathématiques, quai des Augustins, n° 57.

1807.

Traduction française : 1807

RECHERCHES

Carl Friedrich Gauss'

Untersuchungen über höhere Arithmetik.

(Disquisitiones arithmeticae. Theorematis arithmetici demonstratio nova. Summatio quarundam serierum singularium. Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae. Theoria residuorum biquadraticorum, commentatio prima et secunda. Etc.)

Deutsch herausgegeben

von

H. Maser.

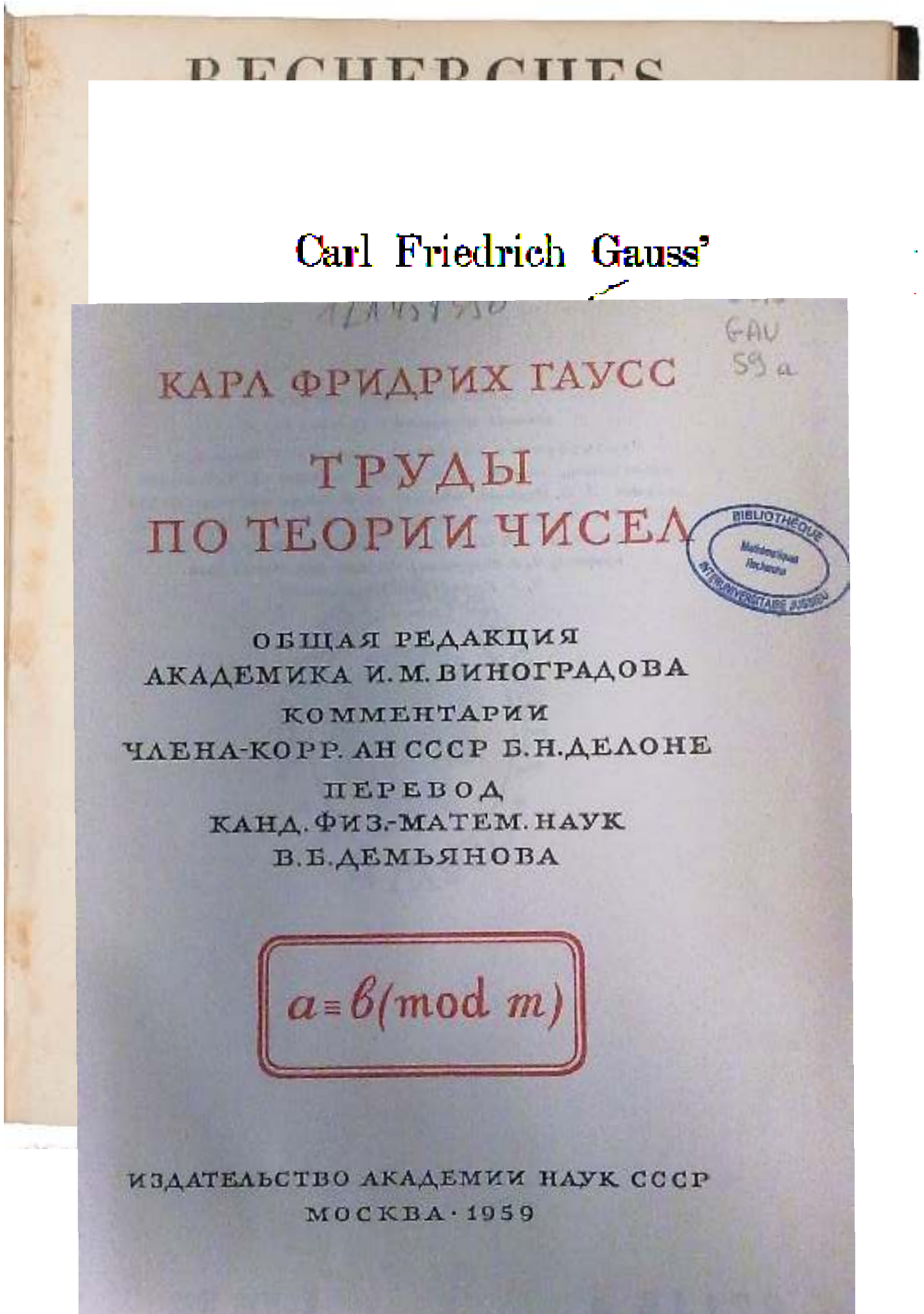
Berlin.

Verlag von Julius Springer.

1889.

Traduction française : 1807

Traduction allemande : 1889



Traduction française : 1807

Traduction allemande : 1889

Traduction russe : 1959

DISQUISITIONES ARITHMETICAE

by Carl Friedrich Gauss

Translated by Arthur A. Clarke, S.J.

NEW HAVEN AND LONDON, YALE UNIVERSITY PRESS, 1966

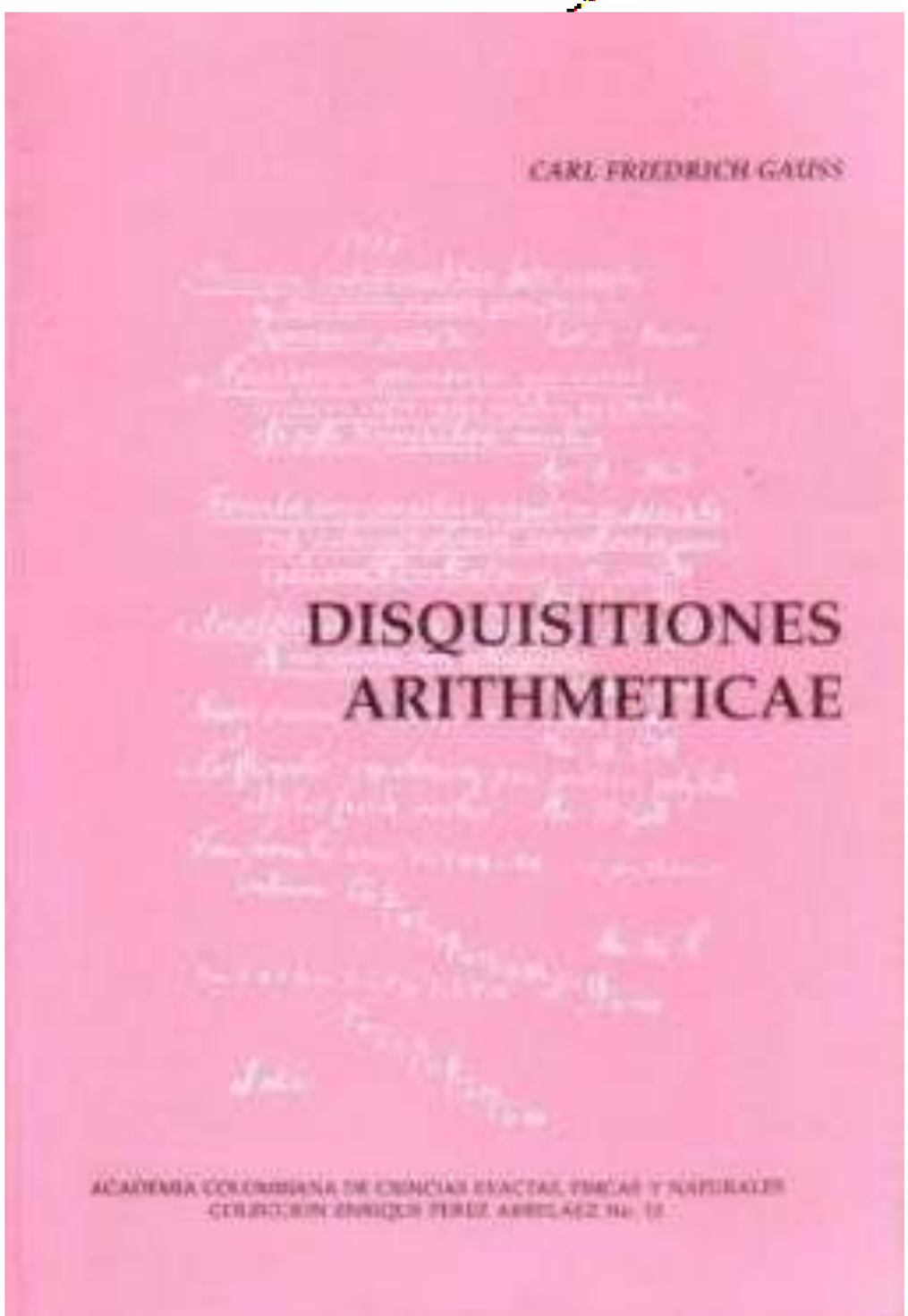
Traduction française : 1807

Traduction allemande : 1889

Traduction russe : 1959

Traduction anglaise : 1966

Carl Friedrich Gauss'



Traduction française : 1807

Traduction allemande : 1889

Traduction russe : 1959

Traduction anglaise : 1966

Traduction castillane : 1995

Traduction française : 1807

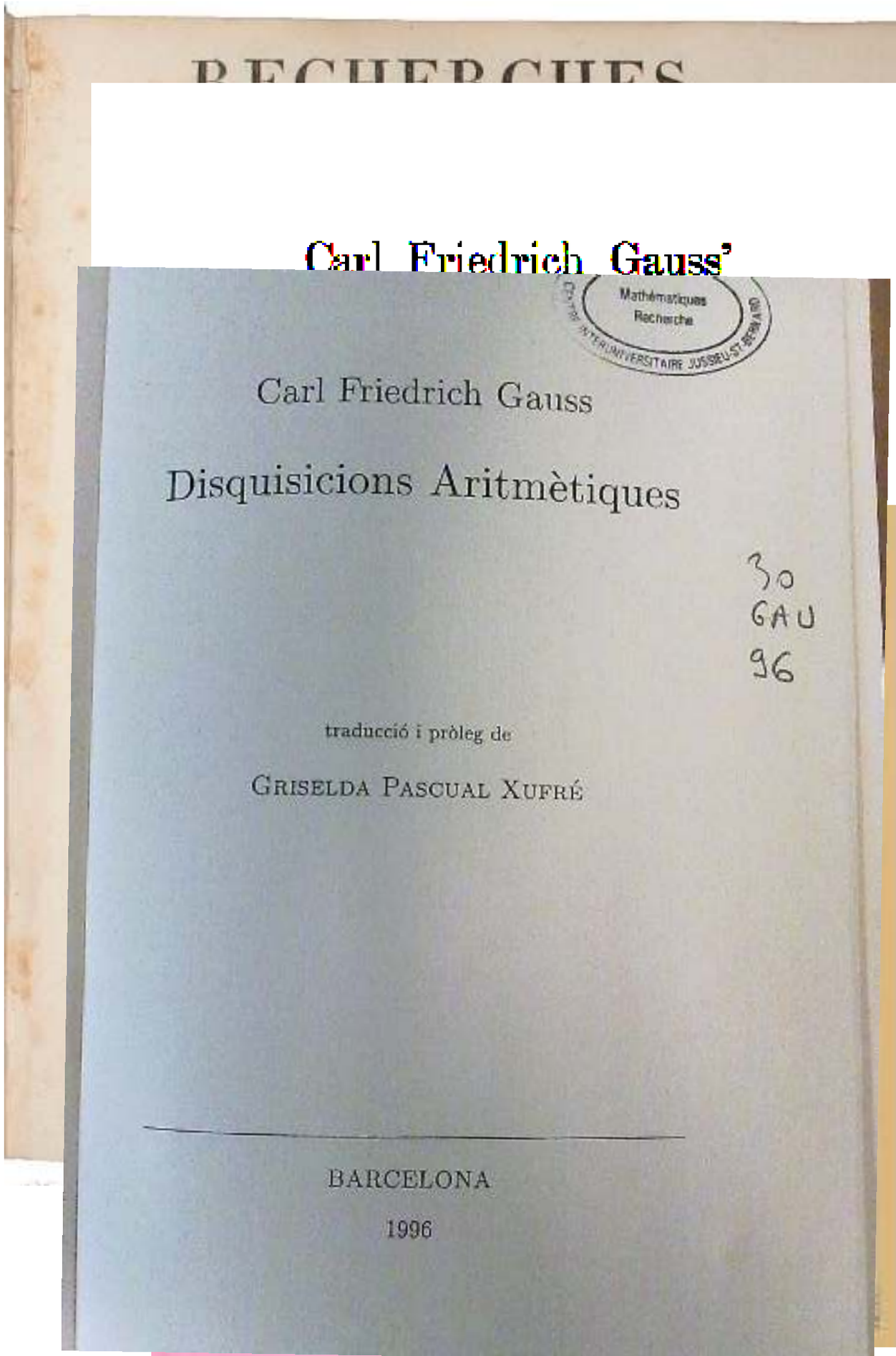
Traduction allemande : 1889

Traduction russe : 1959

Traduction anglaise : 1966

Traduction castillane : 1995

Traduction japonaise : 1995



Traduction française : 1807

Traduction allemande : 1889

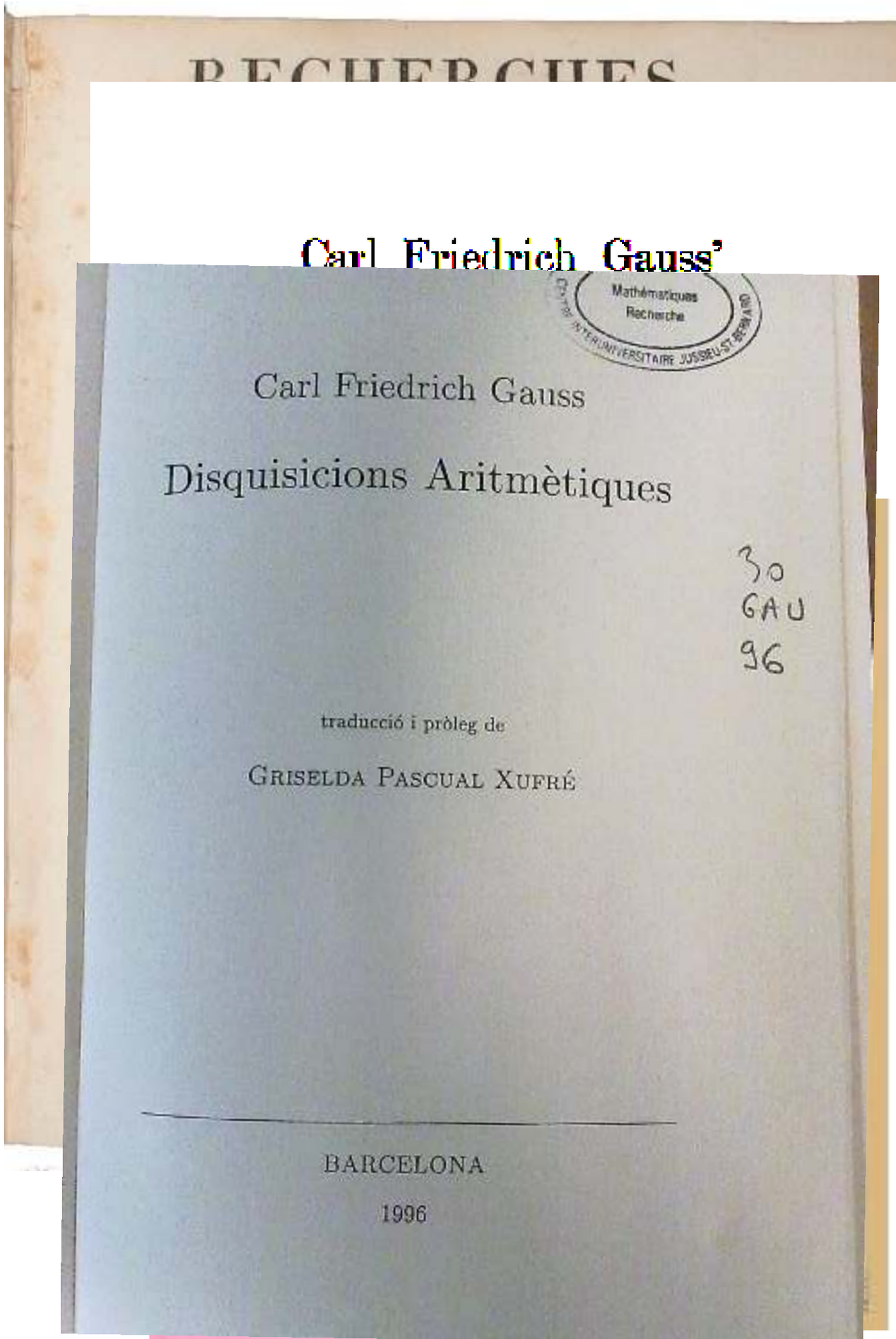
Traduction russe : 1959

Traduction anglaise : 1966

Traduction castillane : 1995

Traduction japonaise : 1995

Traduction catalane : 1996



Traduction française : 1807

Traduction allemande : 1889

Traduction russe : 1959

Traduction anglaise : 1966

Traduction castillane : 1995

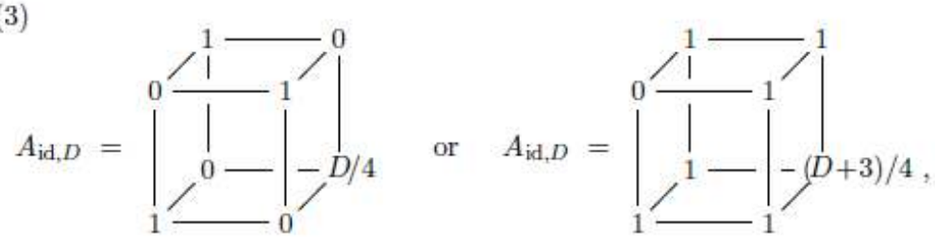
Traduction japonaise : 1995

Traduction catalane : 1996

Traduction chinoise : 2019

in accordance with whether $D \equiv 0 \pmod 4$ or $D \equiv 1 \pmod 4$. That $Q_{\mathrm{id},D}$ satisfies the condition required of it follows from the triply-symmetric cubes

(3)



whose three associated quadratic forms are all given by $Q_{\mathrm{id},D}$ (as defined by (2)).

Indeed, if the identity element $Q_{\mathrm{id},D}$ is given as in (2), then the group law defined by Theorem 1 is equivalent to Gauss composition! Thus Theorem 1 gives a very short and simple description of Gauss composition; namely, it implies that the group defined by Gauss can be obtained simply by considering the free group generated by all primitive quadratic forms of a given discriminant D, modulo the relation $Q_{\mathrm{id},D} = 0$ and modulo all relations of the form $Q_1^A + Q_2^A + Q_3^A = 0$ where Q_1^A, Q_2^A, Q_3^A form a triplet of primitive quadratic forms arising from a cube A of discriminant D.

In Section 3.3 we give a proof of Theorem 1, and of its equivalence with Gauss composition, using the language of ideal classes. An alternative proof, not using ideal classes, is given in the appendix.

We use $(\mathrm{Sym}^2\mathbb{Z}^2)^*$ to denote the lattice of integer-valued binary quadratic forms[2], and we use $\mathrm{Cl}((\mathrm{Sym}^2\mathbb{Z}^2)^*; D)$ to denote the set of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of primitive binary quadratic forms of discriminant D equipped with the above group structure.

2.3. *Composition of* $2\times2\times2$ *cubes.* Theorem 1 actually implies something stronger than Gauss composition: not only do the primitive binary quadratic forms of discriminant D form a group, but the cubes of discriminant D—that give rise to triples of primitive quadratic forms—themselves form a group.

To be more precise, let us say a cube A is *projective* if the forms Q_1^A, Q_2^A, Q_3^A are primitive, and let us denote by $[A]$ the Γ-equivalence class of A. Then we have the following theorem.

[2]Gauss actually considered only the sublattice $\mathrm{Sym}^2\mathbb{Z}^2$ of binary forms whose corresponding symmetric matrices have integer entries. From the modern point of view, however, it is more natural to consider the "dual lattice" $(\mathrm{Sym}^2\mathbb{Z}^2)^*$ of binary quadratic forms having integer coefficients. This is the point of view we adopt.

M. Bhargava, Higher composition laws: a new view on Gauss composition..., *Annals of maths*, 2004

Theorem 1 gives a very short and simple description of Gauss composition…

Une histoire usuelle : les D.A. et la théorie algébrique des nombres

In 1801 Gauss published his *Disquisitiones arithmeticae*, the book that created modern algebraic number theory.

Princeton Companion to Mathematics, 2008, p. 756

Les D.A. : théorie des nombres, mais pas seulement

- Théorie de Pfaff des équations aux dérivées partielles (Jacobi)
- Théorie des groupes et des équations algébriques (Galois)
- Cryptographie (Lucas, Lehmer, Shanks)
- Géométrie (diophantienne) (Poincaré)
- etc

Evariste Galois, Lettre à Auguste Chevalier, 1832

Lors donc qu'on aura épuisé sur le groupe d'une équation tout ce qu'il y a de décompositions propres possibles sur ce groupe, on arrivera à des groupes qu'on pourra transformer, mais dont les permutations seront toujours en même nombre.

Si ces groupes ont chacun un nombre premier de permutations, l'équation sera soluble par radicaux; sinon, non.

Le plus petit nombre de permutations que puisse avoir un groupe indécomposable, quand ce nombre n'est pas premier, est 5.4.3.

2°. Les décompositions les plus simples sont celles qui ont lieu par la méthode de M. Gauss.

Comme ces décompositions sont évidentes, même dans la forme actuelle du groupe de l'équation, il est inutile de s'arrêter longtemps sur cet objet.

Quelles décompositions sont praticables sur une équation qui ne se simplifie pas par la méthode de M. Gauss?

J'ai appelé *primitives* les équations qui ne peuvent se simplifier par la méthode de M. Gauss; non que ces équations soient réellement indécomposables, puisqu'elles peuvent même se résoudre par radicaux.

La méthode de M. Gauss

Les coniques qui admettent un point rationnel forment donc une seule classe, et cette classe comprend également toutes les droites. Reconnaître si une conique admet un point rationnel, c'est un problème que Gauss nous a enseigné à résoudre, dans son Chapitre des *Disquisitiones*, intitulé *Representatio ciffræ*.

Les coniques qui n'ont pas de point rationnel se répartissent en plusieurs classes et les conditions de cette répartition se déduisent immédiatement des principes de ce même Chapitre de Gauss.

Considérons maintenant une cubique unicursale (à coefficients rationnels), cette cubique a un point double qui, étant unique, est forcément rationnel. Soit C ce point double, je dis que notre cubique est équivalente à une droite. En effet, soit D une droite rationnelle quelconque, nous pouvons faire correspondre au point M de la cubique un point M_1 de la droite D, de telle façon que la droite MM_1 passe en C.

Les mêmes principes sont applicables à une courbe unicursale quelconque. Soit $f = 0$ une courbe unicursale rationnelle de degré m; elle aura $\frac{(m-1)(m-2)}{2}$ points doubles. Par ces

$$\frac{(m-1)(m-2)}{2}$$

points doubles, je puis faire passer ∞^{m-2} courbes de degré $m-2$. Comme nos $\frac{(m-1)(m-2)}{2}$ points doubles sont les seuls points doubles d'une courbe à coefficients rationnels, toute fonction symétrique de leurs coordonnées sera rationnelle.

D'où il suit que je pourrai faire passer par ces points doubles et par $m-2$ points rationnels pris à volonté dans le plan une courbe de degré $m-2$, et une seule, et que *cette courbe sera rationnelle* (je veux dire à coefficients rationnels).

L'équation générale des courbes de degré $m-2$ passant par les points doubles sera donc de la forme suivante

$$\alpha_1\varphi_1 + \alpha_2\varphi_2 + \ldots + \alpha_{m-1}\varphi_{m-1} = 0,$$

les α étant des coefficients arbitraires et les φ étant des polynomes en-

H. Poincaré, Propriétés arithmétiques des courbes algébriques, JMPA, 1901

Reconnaître si une conique admet un point rationnel, c'est un problème que Gauss nous a enseigné à résoudre dans son chapitre des *Disquisitiones* intitulé …

[1949b] Numbers of solutions of equations in finite fields

The equations to be considered here are those of the type

$$(1) \qquad a_0x_0^{n_0} + a_1x_1^{n_1} + \cdots + a_rx_r^{n_r} = b.$$

Such equations have an interesting history. In art. 358 of the *Disquisitiones* [1 a],[1] Gauss determines the Gaussian sums (the so-called cyclotomic "periods") of order 3, for a prime of the form $p=3n+1$, and at the same time obtains the numbers of solutions for all congruences $ax^3-by^3\equiv 1 \pmod p$. He draws attention himself to the elegance of his method, as well as to its wide scope; it is only much later, however, viz. in his first memoir on biquadratic residues [1b], that he gave in print another application of the same method; there he treats the next higher case, finds the number of solutions of any congruence $ax^4-by^4\equiv 1 \pmod p$, for a prime of the form $p=4n+1$, and derives from this the biquadratic character of 2 mod p, this being the ostensible purpose of the whole highly ingenious and intricate investigation. As an incidental consequence ("*coronidis loco*," p. 89), he also gives in substance the number of solutions of any congruence $y^2\equiv ax^4-b \pmod p$; this result includes as a special case the theorem stated as a conjecture ("*observatio per inductionem facta gravissima*") in the last entry of his *Tagebuch* [1c];[2] and it implies the truth of what has lately become known as the Riemann hypothesis, for the function-field defined by that equation over the prime field of p elements.

Gauss' procedure is wholly elementary, and makes no use of the Gaussian sums, since it is rather his purpose to apply it to the determination of such sums. If one tries to apply it to more general cases, however, calculations soon become unwieldy, and one realizes the necessity of inverting it by taking Gaussian sums as a starting point. The means for doing so were supplied, as early as 1827, by Jacobi, in a letter to Gauss [2a] (cf. [2b]). But Lebesgue, who in 1837 devoted two papers [3a, b] to the case $n_0=\cdots=n_r$ of equation (1), did not

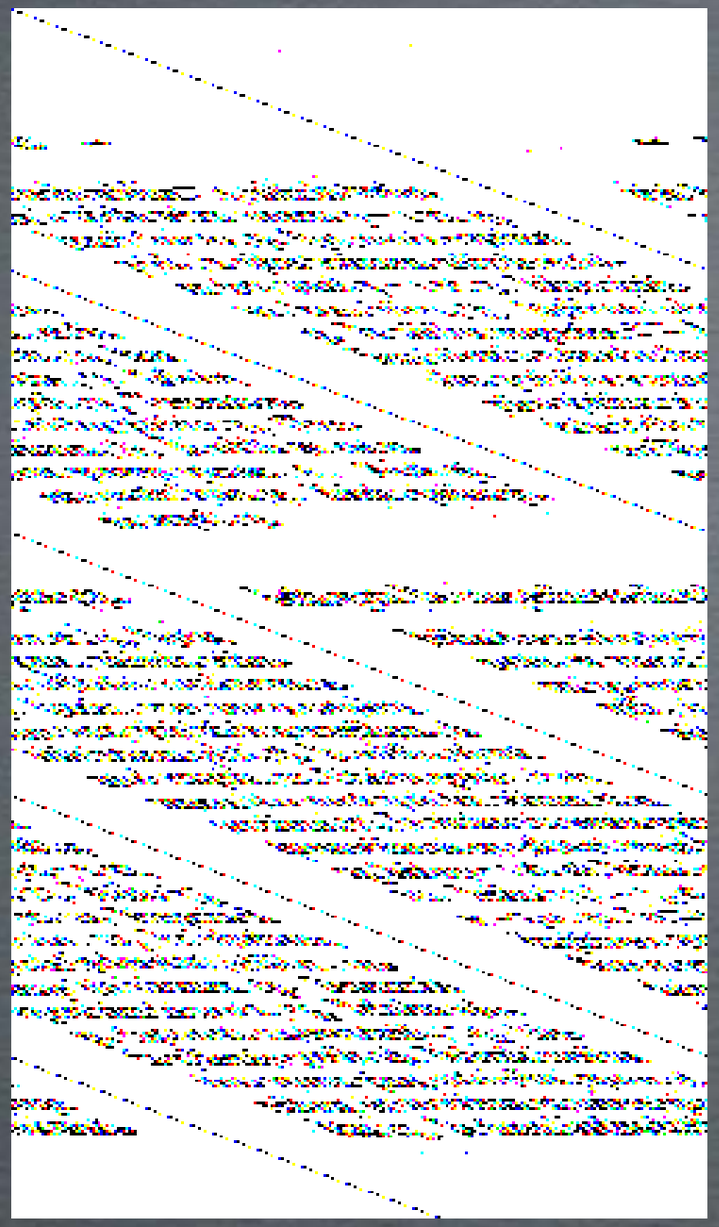
Received by the editors October 2, 1948; published with the invited addresses for reasons of space and editorial convenience.

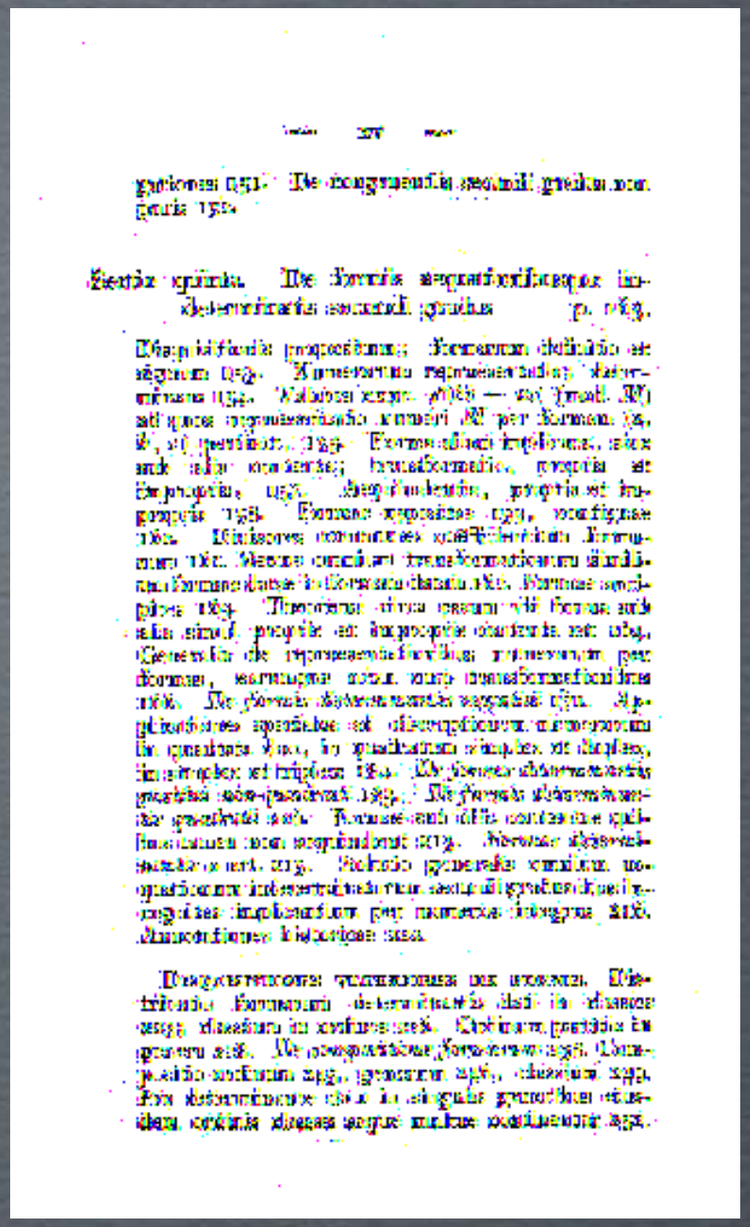
[1] Numbers in brackets refer to the bibliography at the end of the paper.

[2] It is surprising that this should have been overlooked by Dedekind and other authors who have discussed that conjecture (cf. M. Deuring, Abh. Math. Sem. Hamburgischen Univ. vol. 14 (1941) pp. 197–198).

A.Weil, Numbers of solutions of equations in finite fields, *Bulletin AMS*, 1949

Dans l'art. 358 des *Disquisitiones*, Gauss détermine les sommes de Gauss d'ordre 3, pour un nombre premier de la forme p=3n+1 et en même temps obtient les nombres de solutions pour toutes les congruences $ax^3-by^3 \equiv 1 \pmod p$

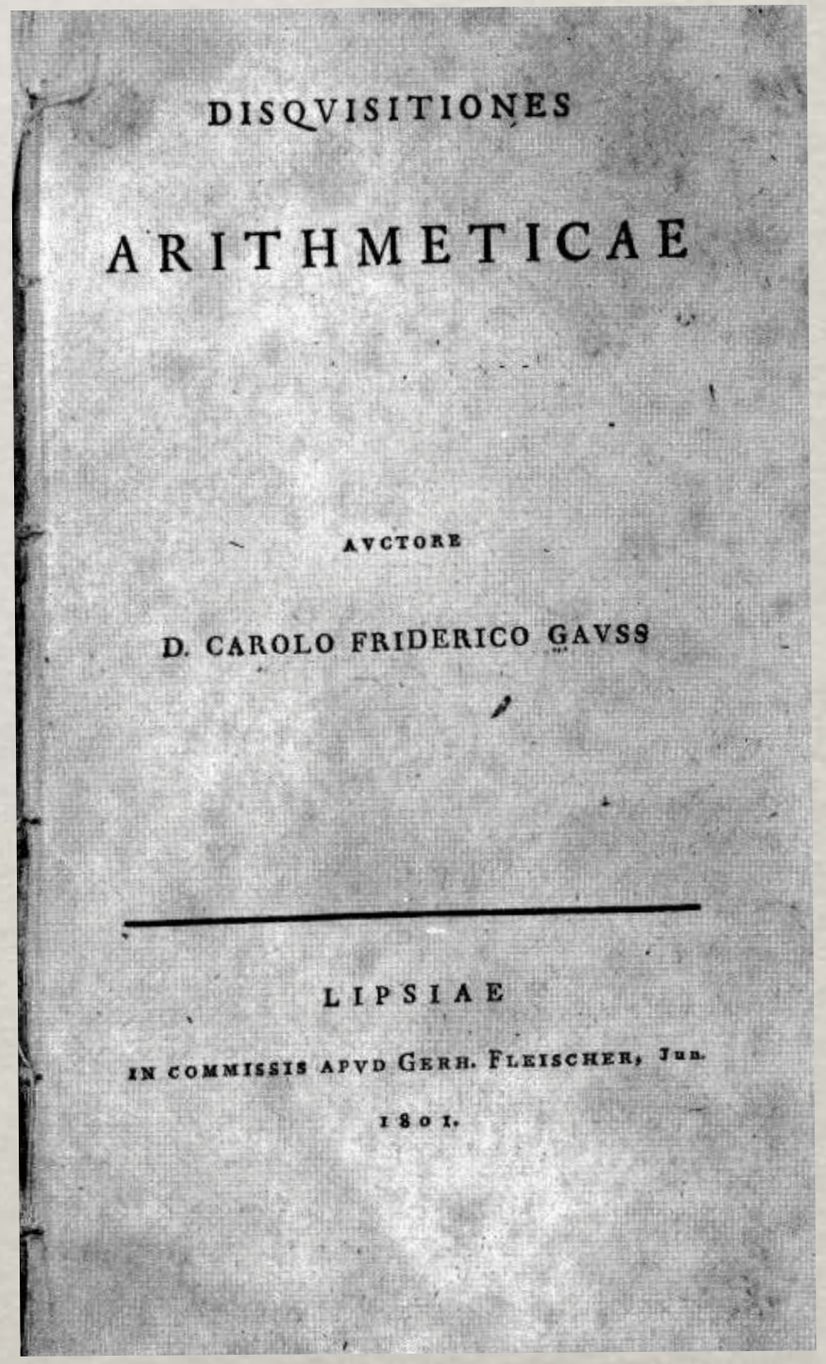




LA STRUCTURE DES DISQUISITIONES ARITHMETICAE

LES D.A. EN 1801

- “Les entiers… constituent l’objet propre de l’arithmétique.”
- 665 pages
- 355 articles
- 7 sections (“les sept sceaux”)


DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

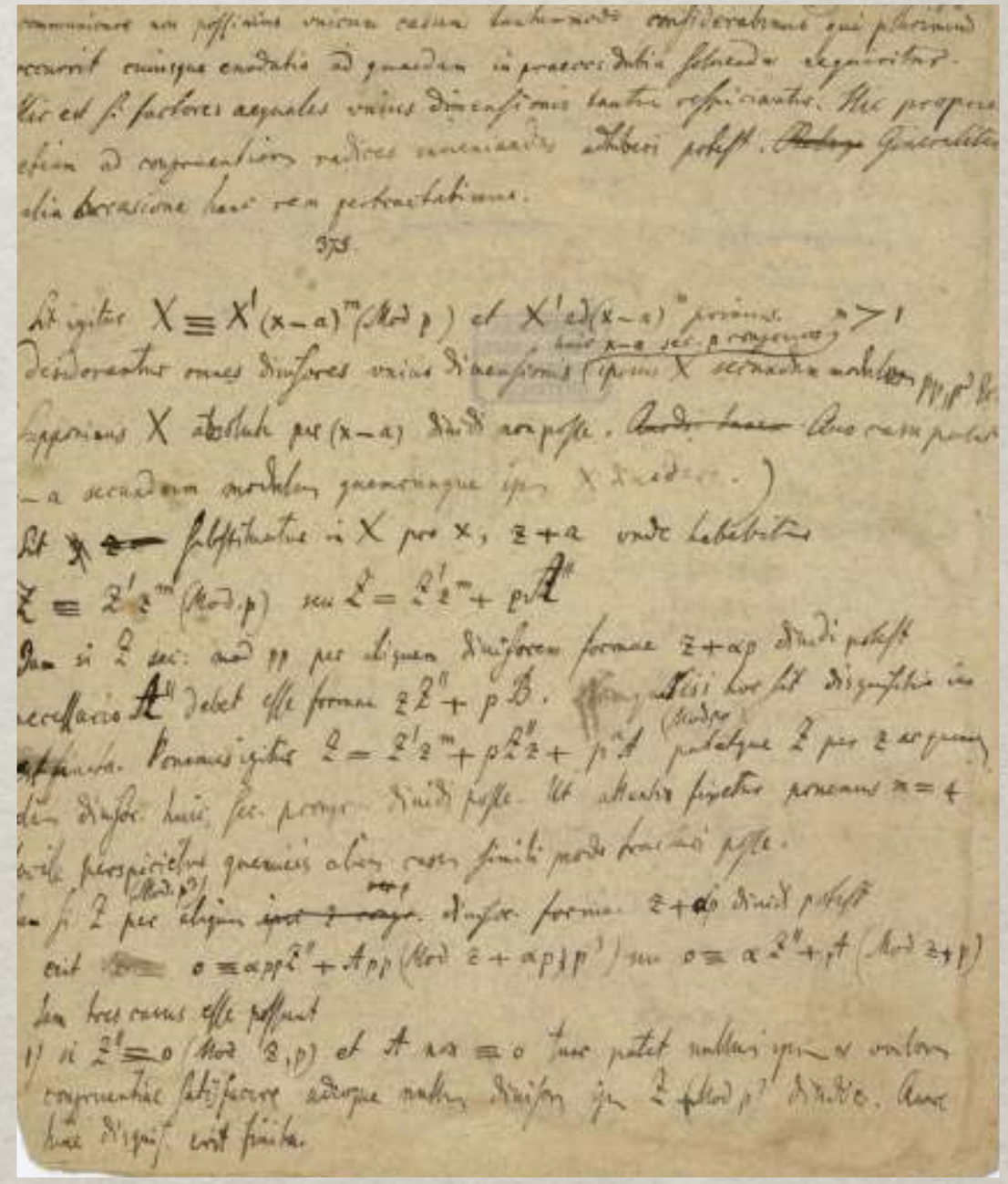
LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, JUN.

1801.

Les D.A. vus par Gauss

- résultats fondamentaux obtenus dès 1796
- première version en 1797
- 8 sections
- impression (difficile) à partir de 1798



- Nombres congrus
- Congruences du premier degré
- Résidus de puissances
- Congruences du second degré
- Formes et équations indéterminées du second degré
- Applications variées
- Sur les équations déterminant les divisions du cercle

- Nombres congrus
- Congruences du premier degré
- Résidus de puissances
- Congruences du second degré
- Formes et équations indéterminées du second degré
- Applications variées
- Sur les équations déterminant les divisions du cercle

Congruences

1. Si un nombre a divise la différence des nombres b et c, b et c sont dits *congrus* suivant a, sinon *incongrus*. a s'appellera le module ; chacun des nombres b et c, *résidus* de l'autre dans le premier cas, et *non résidus* dans le second.

Nous désignerons dorénavant la congruence de deux nombres par ce signe $\equiv$, en y joignant, lorsqu'il sera nécessaire, le module renfermé entre parenthèses; ainsi $-16 \equiv 9$ (mod. 5), $-7 \equiv 15$ (mod. 11) (*).

«* Nous avons adopté ce signe à cause de la grande analogie qui existe entre l'égalité et la congruence. »

- Compatibilité avec les quatre opérations arithmétiques
- Critères de divisibilité, résolution d'équations aux congruences du premier degré

Congruences

- étude des progressions géométriques *1*, *a*, a^2, ... modulo un nombre premier *p*
- Petit théorème de Fermat : si $(a, p)=1$

$$a^{p-1} \equiv 1 \pmod{p}$$

- “Il existe des nombres dont aucune puissance plus petite que *p-1* est congruente à 1 modulo *p*” [=> en termes actuels : (Z/pZ)* is cyclic]
- “Cet exemple nous fournit un exemple remarquable de la circonspection dont on a besoin dans la théorie des nombres pour ne pas regarder comme démontrées des choses qui ne le sont pas”.

SECTION SECONDE. *Des Congruences du premier degré.*

Théorèmes préliminaires sur les nombres premiers, les diviseurs, etc. n° 13 — 23
Résolution des congruences du premier degré . . . . . 24 — 31
De la recherche d'un nombre congru à des nombres donnés suivant des modules donnés . . . . . 32 — 36
Congruences du premier degré à plusieurs inconnues 37
Différens théorèmes . . . . . 38 et suiv.

SECTION TROISIÈME. *Des résidus des puissances.*

Les résidus des termes d'une progression géométrique qui commence par l'unité, forment une suite périodique . . . . . n° 45 — 48

Des modules qui sont des nombres premiers.

Si le module est un nombre premier p, le nombre des termes de la période divise nécessairement $p-1$ 49
Théorème de *Fermat*. 50, 51
A combien de nombres répondent les périodes dont le nombre des termes est un diviseur donné de $p-1$ . . . . . 52 — 56
Racines primitives, *bases*, *indices* 57
Algorithme des indices 58, 59
Des racines de la congruence $x^n \equiv A$. . . . . 60 — 68
Relation entre les indices pour différens systèmes. . . . . 69 — 71
Bases choisies pour des usages particuliers 72
Méthode pour trouver les racines primitives 73, 74
Divers théorèmes sur les périodes et les racines primitives. . . . . 75 — 81

SECTION SECONDE. *Des Congruences du premier degré.*

Théorèmes préliminaires sur les nombres premiers, les diviseurs, etc. n° 13 — 23
Résolution des congruences du premier degré . . . . . 24 — 31
De la recherche d'un nombre congru à des nombres donnés suivant des modules donnés . . . . . 32 — 36
Congruences du premier degré à plusieurs inconnues 37
Différens théorèmes . . . . . 38 et suiv.

SECTION TROISIÈME. *Des résidus des puissances.*

Les résidus des termes d'une progression géométrique qui commence par l'unité, forment une suite périodique . . . . . n° 45 — 48

Des modules qui sont des nombres premiers.

Si le module est un nombre premier p, le nombre des termes de la période divise nécessairement $p-1$ 49
Théorème de *Fermat*. 50, 51
A combien de nombres répondent les périodes dont le nombre des termes est un diviseur donné de $p-1$ . . . . . 52 — 56
Racines primitives, bases, indices 57
Algorithme des indices 58, 59
Des racines de la congruence $x^n \equiv A$. . . . . 60 — 68
Relation entre les indices pour différens systèmes. . . . . 69 — 71
Bases choisies pour des usages particuliers 72
Méthode pour trouver les racines primitives 73, 74
Divers théorèmes sur les périodes et les racines primitives. . . . . 75 — 81

Des conditions $z \equiv -4 \bmod 5$, $z \equiv -4 \bmod 7$, on tire immédiatement $z \equiv -4 \bmod 35$, d'où elles dérivent. Il s'ensuit qu'il n'est pas indifférent, quant à la brièveté du calcul, de rejeter l'une ou l'autre des conditions équivalentes. Mais il n'entre pas dans notre plan de parler de ces détails ni d'autres artifices pratiques, que l'usage apprend mieux que les préceptes.

Congruences

- résidus quadratiques a modulo p (= résidus des nombres carrés modulo p)

$$a \equiv x^2 \pmod{p}$$

- -1 est un résidu quadratique pour p =4n+1 ; -2 est un résidu quadratique pour p=8n+3, etc.

- Loi de réciprocité quadratique (“Théorème fondamental”) : énoncé et (première) preuve rigoureuse, par récurrence et étude cas par cas

Congruences

- Loi de réciprocité quadratique (“Théorème fondamental”) : énoncé et (première) preuve rigoureuse, par récurrence et étude cas par cas

Tout nombre qui, pris positivement, est résidu ou non-résidu de p, *aura, pour résidu ou non-résidu,* $+p$ *ou* $-p$, *selon que* p *sera de la forme* $4n+1$ *ou* $4n+3$.

Comme presque tout ce qu'on peut dire sur les résidus quadratiques est une suite de ce théorème, la dénomination du *théorème fondamental* dont nous nous servirons dorénavant, ne sera pas déplacée.

Congruences

$$\left(\frac{p}{p}\right) = 0$$

$$\left(\frac{p}{q}\right) = 1$$ si p est résidu quadratique mod q

$$\left(\frac{p}{q}\right) = -1$$ si p est non résidu quadratique mod q

Loi de réciprocité quadratique (un peu modernisée !)

Si p et q sont deux nombres premiers impairs,

$$\left(\frac{\pm p}{q}\right) = \left(\frac{q}{p}\right)$$

avec $+p$ si $p = 4n + 1$ et $-p$ si $p = 4n + 3$.

- Nombres congrus
- Congruences du premier degré
- Résidus de puissances
- Congruences du second degré
- Formes et équations indéterminées du second degré
- Applications variées
- Sur les équations déterminant les divisions du cercle

Formes quadratiques

- “The arithmetical theory of forms…only yielded their cause of being when turned over in the blow-pipe flame of Gauss's transcendent genius” (J.J. Sylvester, 1869)

- Etude de : $ax^2+2bxy+cy^2$, avec a, b, c entiers

- Question (classique) 1: quels nombres entiers peuvent-ils être représentés par une forme donnée ? E.g. : est-ce que 21 ou 101 est une somme de deux carrés, x^2+y^2 ? Comment trouver ces carrés s’ils existent ?

- Question 2 : classifier les formes à un changement de variables linéaire, inversible, à coefficients entiers, près.

$x=ux'+vy'$, $y=u'x'+v'y'$, avec u, u', v, v' entiers et $uv'-u'v=\pm 1$

Formes quadratiques

- Question 2 (classification des formes à $GL_2(\mathbf{Z})$ près) devient la plus importante
- $ax^2+2bxy+cy^2$, avec a, b, c entiers => (a, b, c)
  - importance pour la classification de l'invariant b^2-ac (="déterminant")
  - nombre fini de classes de formes équivalentes à déterminant fixé
  - bons *représentants* de chaque classe (formes réduites).

  Par exemple pour $b^2-ac<0$, une forme réduite est telle que

$$0< a \leq 2\sqrt{(ac-b^2)}/3,\ 0\leq b \leq a/2 \leq c$$

- composition des formes

Composition des formes

Modèle : $(xx' - Nyy')^2 + N(xy' + yx')^2 = (x^2 + Ny^2) \cdot (x'^2 + Ny'^2)$

Pour Gauss: $F(X,Y) = AX^2+2BXY+CY^2$ est composé des formes f et f' si $F(X,Y)=f(x,y)\ f'(x',y')$, avec
$X= pxx'+p'xy'+p''x'y+p'''yy'$, $Y= qxx'+q'xy'+q''x'y+q'''yy'$
et des conditions sur p, p', p'', etc.

Ceci définit une multiplication sur les classes de formes

"La théorie de la multiplication des classes a une forte affinité avec celle développée dans la Section III [= classes de résidus des nombres premiers à p, modulo p, i. e. (Z/pZ)*]"

Formes quadratiques

- Question 2 : classification des formes
  - importance de l'invariant b^2-ac (="déterminant")
  - classes de formes équivalentes à déterminant fixé
  - bons *représentants* de chaque classe (formes réduites)
- composition des formes (=> structure multiplicative sur des classes des formes avec un déterminant donné)
- liens avec équation de Pell-Fermat x^2-Ny^2=1, représentation des nombres par les formes, équations indéterminées
- classification plus poussée des formes : ordre, genre…(Gauss introduit les formes quadratiques ternaires pour cela), avec des conjectures sur les nombres de classes (certaines toujours ouvertes)
- applications : 2e démonstration du théorème fondamental, démonstration que tout nombre du type 8n+3 est une somme de 3 carrés, …

- Nombres congrus
- Congruences du premier degré
- Résidus de puissances
- Congruences du second degré
- Formes et équations indéterminées du second degré
- Applications variées
- Sur les équations déterminant les divisions du cercle

Applications

- décomposition des fractions
- calculs explicites sur les congruences
- tests de primalité et factorisation : une méthode par congruences, une autre par les formes

Fractions

- fin 17e (cadre =enseignement unifié de l'algèbre et de l'arithmétique), intérêt pour

$$\frac{1}{41} = 0{,}0243902439024390\ldots$$

$$\frac{1}{7} = 0{,}142857142857142\ldots \frac{2}{7} = 0{,}2857142857\ldots$$

$$\frac{1}{17} = 0{,}0588235294117647058823529411764705 88\ldots$$

d'après M. Bullynck, *Historia Mathematica*, 2009

Fractions

En mécanique, on a depuis longtemps utilisé [ce principe de périodicité] comme source d'invention des machines, parce que chaque retour périodique de transformations peut être engendré par des machines et chaque ordre local dans une série de changements devient périodique.

J. Lambert, 1771, cité d'après M. Bullynck, *Historia Mathematica*, 2009

Fractions

En mécanique, on a depuis longtemps utilisé [ce principe de périodicité] comme source d'invention des machines, parce que chaque retour périodique de transformations peut être engendré par des machines et chaque ordre local dans une série de changements devient périodique.

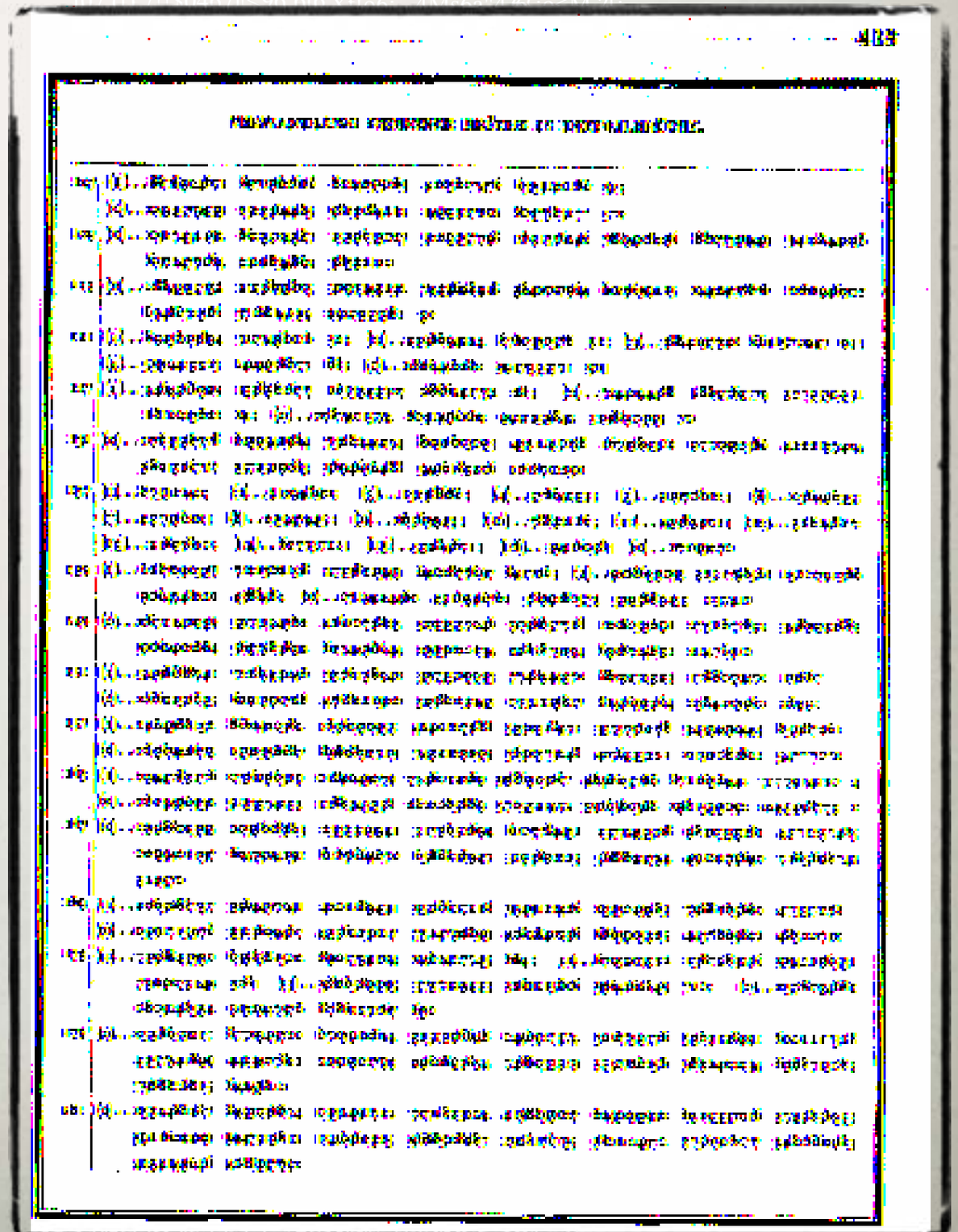
Lambert : lien avec le petit théorème de Fermat,
k/p période maximale (de longueur p-1) si 10 d'indice maximal modulo dénominateur p

J. Lambert, 1771, cité d'après M. Bullynck, Historia Mathematica, 2009

Fractions

Gauss, DA, sect. 6 : selon indice, une ou plusieurs périodes de différentes longueur ; calcul du décalage pour les multiples, etc.

Ex : 12/19 :
10 est racine primitive modulo 19, donc 1 période
ind 12 ≡ 3 mod 18, donc décalage de 3 de la période par rapport à celle de 1/19



M. Bullynck, *Historia Mathematica*, 2009

Primalité et factorisation

- Méthode 1 : Si n est résidu quadratique modulo M, il l'est aussi pour chaque diviseur m de M.

  Donc 1) on liste les résidus quadratiques n_i mod M

  2) chaque m pour lequel un n_i n'est pas résidu quadratique est exclu comme diviseur de M.

  Ex. M = 997 331 : les résidus quadratiques n_i = -6, 13, -14, 17, 37, -53 excluent tous les diviseurs possibles m <127. Finalement 997331 = 127.7853.

	−	+	−	+	+	−
	6	13	14	17	37	53
3	—	—	—		—	—
5	—		—			
7	—		—		—	
11	—				—	
13		—	—	—		—
17		—		—		—
19			—	—		—
23		—	—			—
etc.			etc.			etc.
113		—	—			—
127	—	—	—	—	—	—

- Méthode 2 : M est écrit comme un diviseur d'une forme quadratique $x^2 + Dy^2$.

  Ex : M = 4 272 943 = $x^2 + 286y^2$

  (= $(1113)^2 + 286(103)^2$) est premier

- Nombres congrus
- Congruences du premier degré
- Résidus de puissances
- Congruences du second degré
- Formes et équations indéterminées du second degré
- Applications variées
- Sur les équations déterminant les divisions du cercle

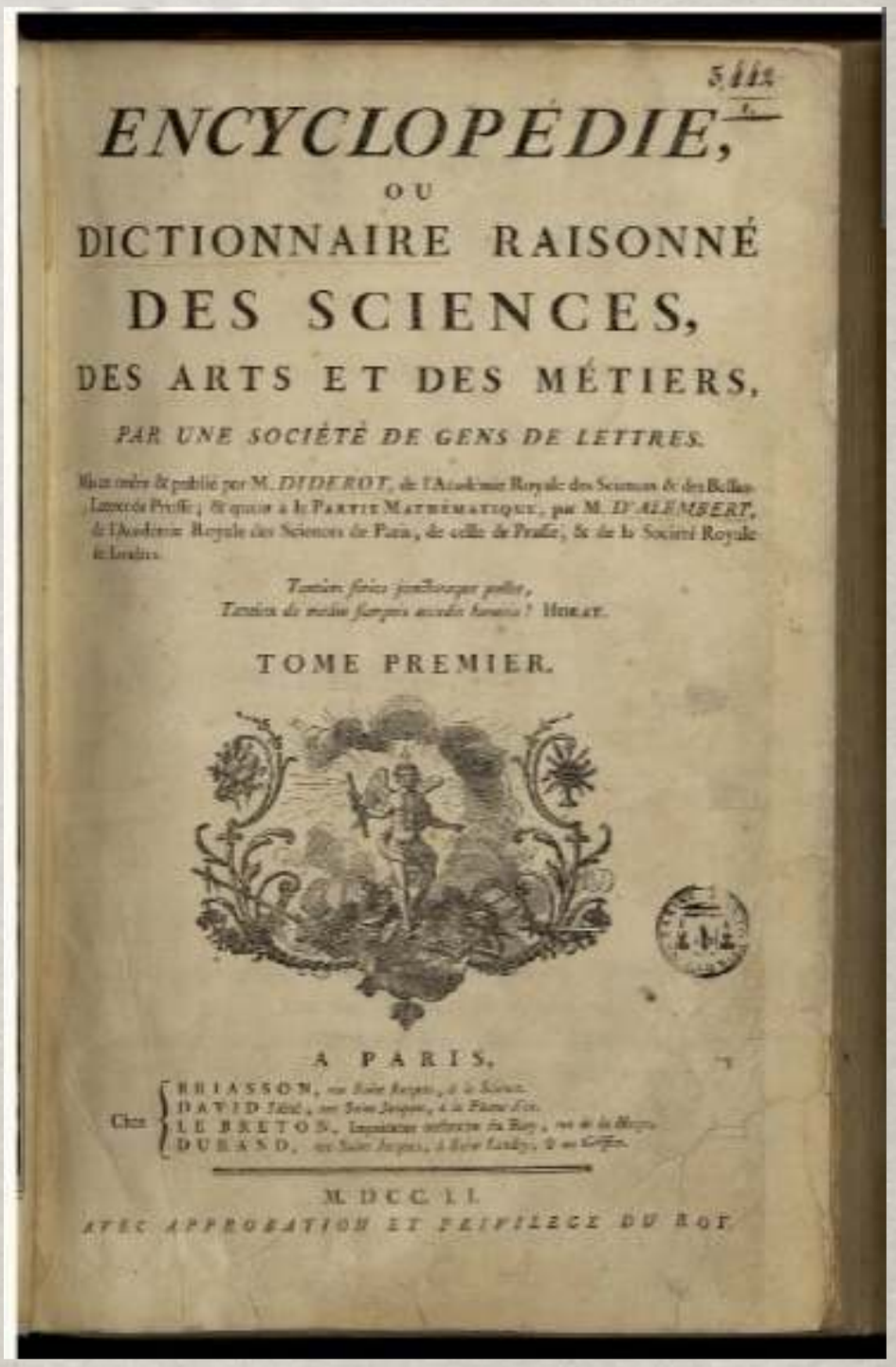
- Nombres congrus
- Congruences du premier degré
- Résidus de puissances
- Congruences du second degré
- Formes et équations indéterminées du second degré
- Applications variées
- Sur les équations déterminant les divisions du cercle

Construction, s. f. Ce mot exprime, en Géométrie, les opérations qu'il faut faire pour exécuter la solution d'un problème. La construction d'une équation, est la méthode d'en trouver les racines par des opérations faites avec la regle & le compas, ou en général par la description de quelque courbe.

[O : d'Alembert, *Encyclopédie*]

EFFECTIF, adj. qui est réel & positif. Dans le Commerce, un payement effectif est celui qui se fait véritablement & en deniers comptans, ou effets équivalens.

[G : Edme François Mallet, *Encyclopédie*]



ENCYCLOPEDIE,

OU

DICTIONNAIRE RAISONNÉ

DES SCIENCES,

DES ARTS ET DES MÉTIERS,

PAR UNE SOCIÉTÉ DE GENS DE LETTRES.

TOME PREMIER.

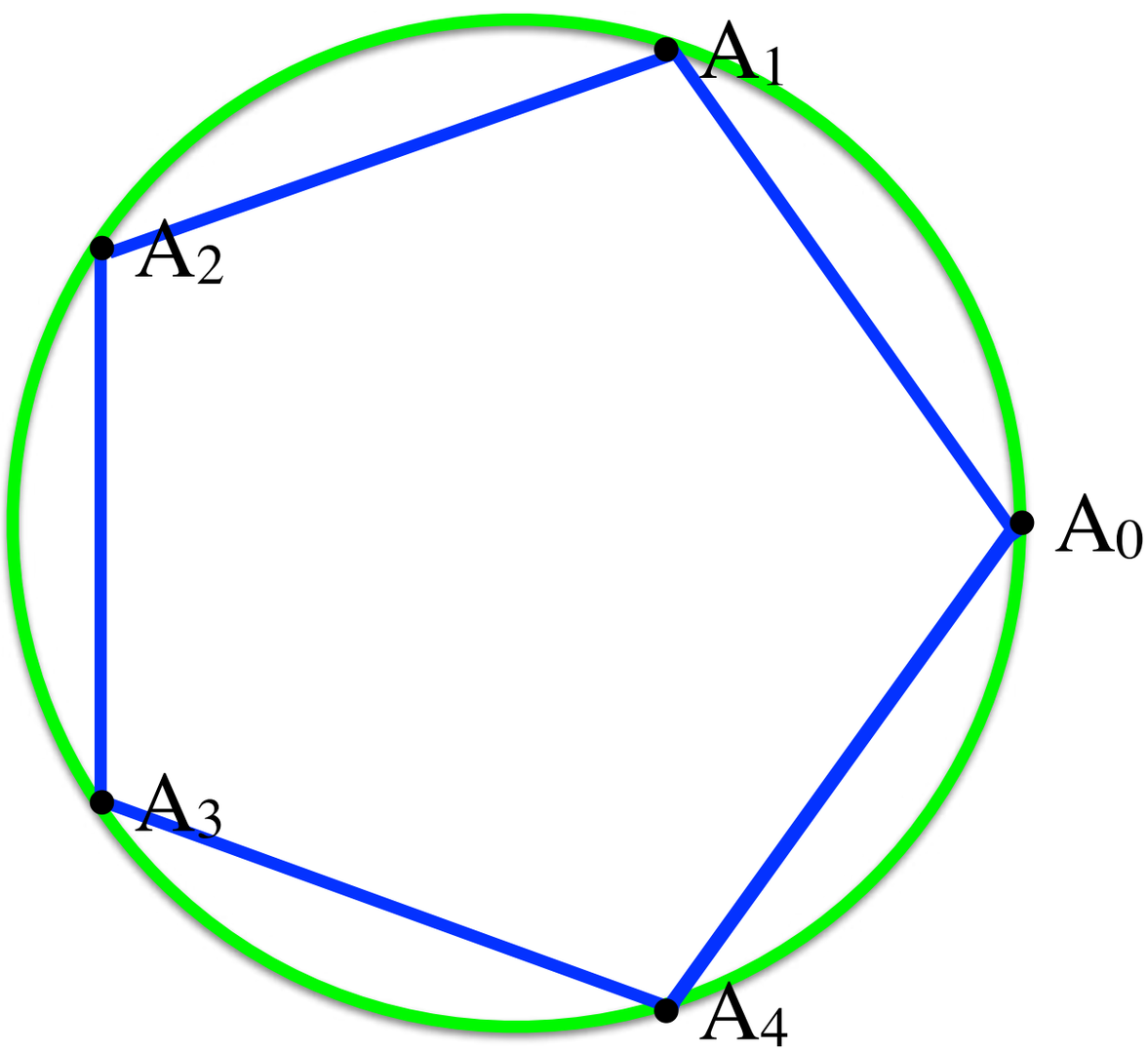
A PARIS,

M. DCC. LI.

AVEC APPROBATION ET PRIVILEGE DU ROI.

http://enccre.academie-sciences.fr/

Inscrire des polygones réguliers dans un cercle à la règle et au compas



A_0 : $(1,0) = \exp(0\pi i/5)$

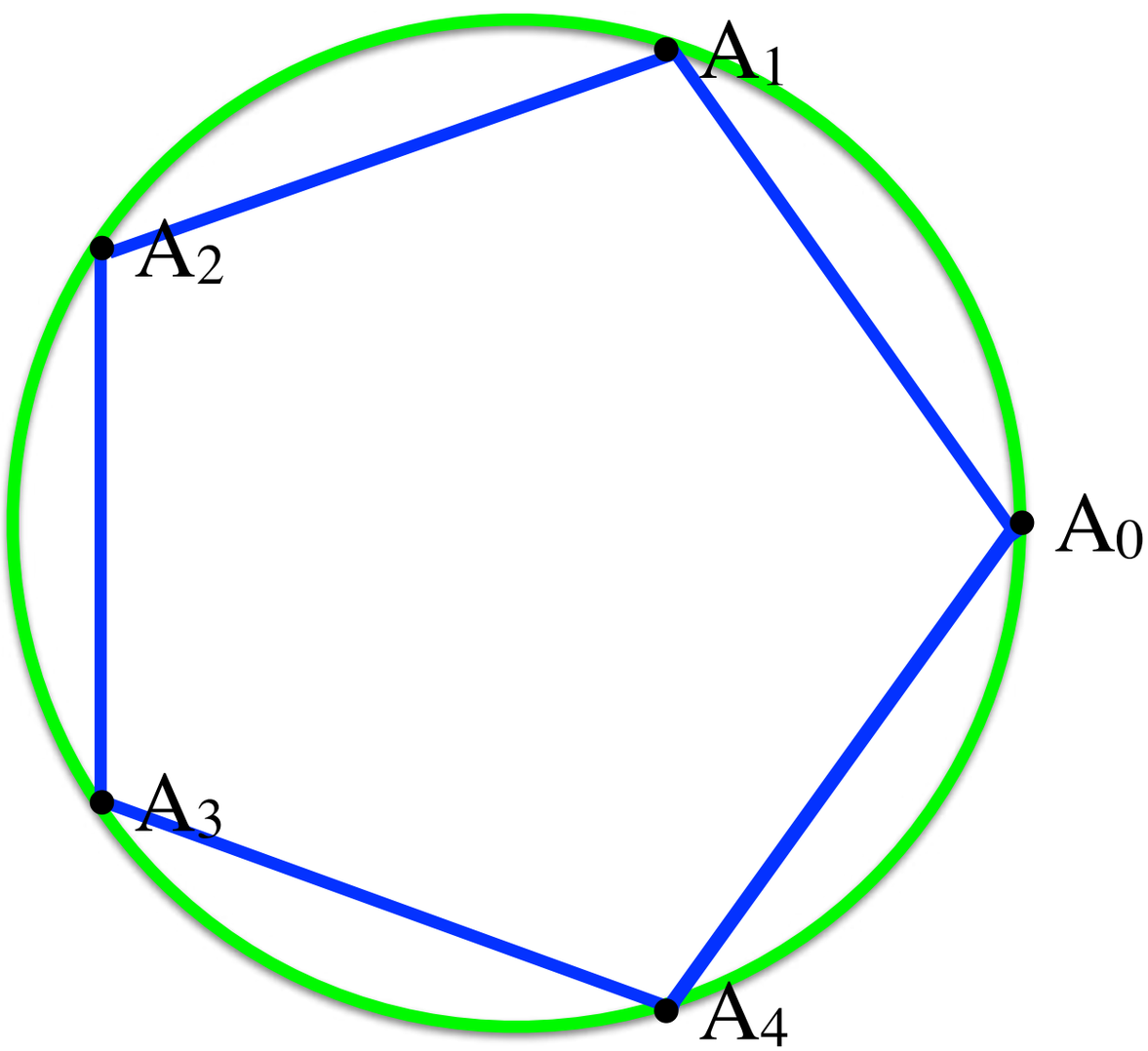
A_1 : $(\cos 2\pi/5, \sin 2\pi/5) = \exp(2\pi i/5)$

A_2 : $(\cos 4\pi/5, \sin 4\pi/5) = \exp(4\pi i/5)$

A_3 : $(\cos 6\pi/5, \sin 6\pi/5) = \exp(6\pi i/5)$

A_4 : $(\cos 8\pi/5, \sin 8\pi/5) = \exp(8\pi i/5)$

Inscrire des polygones réguliers dans un cercle à la règle et au compas



A_0 : $(1,0) = \exp(0\pi i/5)$

A_1 : $(\cos 2\pi/5, \sin 2\pi/5) = \exp(2\pi i/5)$

A_2 : $(\cos 4\pi/5, \sin 4\pi/5) = \exp(4\pi i/5)$

A_3 : $(\cos 6\pi/5, \sin 6\pi/5) = \exp(6\pi i/5)$

A_4 : $(\cos 8\pi/5, \sin 8\pi/5) = \exp(8\pi i/5)$

Construire à la règle et au compas les solutions de $x^5-1=0$

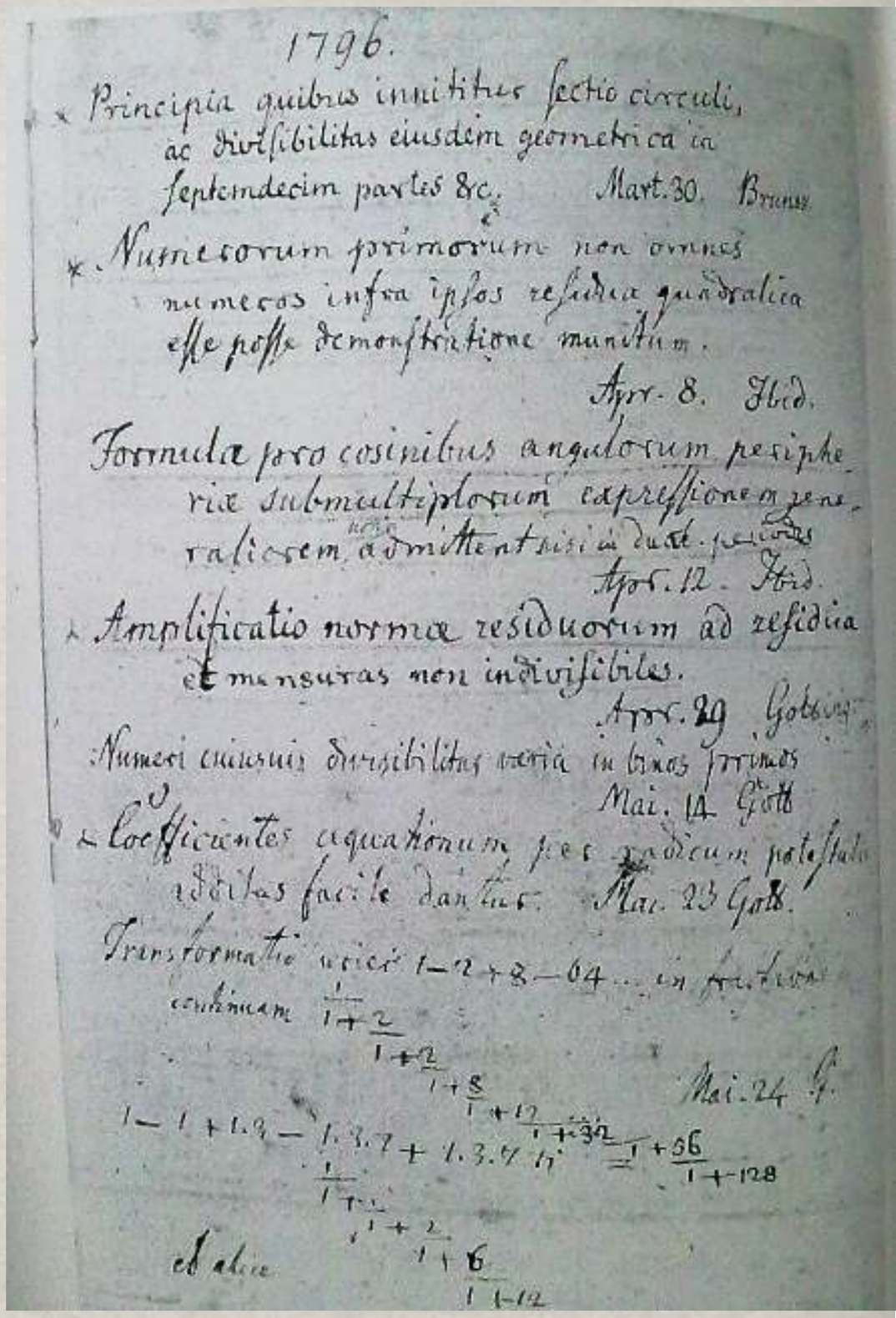
“On trouve donc, en-dessous de 300, les 38 valeurs suivantes pour le nombre N [tel qu’un polygone régulier à N côtés soit inscriptible à la règle et au compas dans un cercle] :
2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272.”

C'était le 29 mars 1796. […] Par une intense réflexion sur la relation entre les racines, sur des bases arithmétiques, j'ai réussi pendant des vacances à Brunswick, le matin de ce jour (avant de sortir du lit) à concevoir cette relation si clairement que je pouvais en faire immédiatement la confirmation numérique dans le cas de l'application particulière au polygone à 17 côtés.

Gauss à Gerling, 6 janvier 1819

C'était le 29 mars 1796. […] Par une intense réflexion sur la relation entre les racines, sur des bases arithmétiques, j'ai réussi pendant des vacances à Brunswick, le matin de ce jour (avant de sortir du lit) à concevoir cette relation si clairement que je pouvais en faire immédiatement la confirmation numérique dans le cas de l'application particulière au polygone à 17 côtés.

Gauss à Gerling, 6 janvier 1819



Première page du journal de Gauss

Division du cercle

- Etude de $(x^p-1)/(x-1)=x^{p-1}+x^{p-2}+\ldots+x+1=0$, p premier >2
- Racines $\zeta^j = \cos 2\pi j/p + i \sin 2\pi j/p$ avec j=1, ...p-1
- Les exposants j peuvent être exprimés comme des puissances d'une racine primitive mod p (=générateur de (Z/pZ)*) => ceci permet de réordonner les racines
- Les nouveaux groupements des racines conduisent à la décomposition graduelle de l'équation en équations de degrés divisant p-1.
- Gauss détermine ainsi quels polygones réguliers peuvent être construits à la règle et au compas : le nombre N de côtés doit être 2^k, ou un nombre premier p tel que $p-1=2^k$ (p est un premier de Fermat), ou un produit $2^k p_1 p_2 \ldots p_r$, avec p_i différents premiers de Fermat.

Cas p=19

$X = x^{18}+x^{17}+\ldots+x+1=0$:

Les racines sont r^j , j = 1, 2, ... 18, avec
$r = \cos 2\pi/19 + i \sin 2\pi/19$

On peut prendre 2 comme racine primitive modulo 19

$j \equiv 2^k \bmod 19$

j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
k	0	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

- Ceci donne une nouvel ordre des racines

$j \equiv 2^k \bmod 19$

j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
k	0	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

j	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

Division du cercle

- Etude de $(x^p-1)/(x-1)=x^{p-1}+x^{p-2}+\ldots+x+1=0$, p premier >2
- Racines $\zeta^j = \cos 2\pi j/p + i \sin 2\pi j/p$ avec j=1, ...p-1
- Les exposants j peuvent être exprimés comme des puissances d'une racine primitive mod p (=générateur de (Z/pZ)*) => réordonne les racines
- Les nouveaux groupements des racines conduisent à la décomposition graduelle de l'équation en équations de degrés divisant p-1
- Gauss détermine ainsi quels polygones réguliers peuvent être construits à la règle et au compas : le nombre n de côtés doit être 2^k, ou un nombre premier p tel que $p-1=2^k$ (p est un premier de Fermat), ou un produit $2^k p_1 p_2 \ldots p_r$, avec p_i différent premiers de Fermat.

- Pour tout diviseur d de 18, Gauss obtient des *périodes* [d, f], en groupant et ajoutant d racines, à partir de r^f.

- Exemple pour d= 6 : on a 3 périodes différentes [6, 1], [6, 2], [6, 4]

j	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

Par exemple : une période regroupe les termes relatifs à k= 1, 4, 7, 10, 13, 16, soit j= 2, 16, 14, 17, 3, 5.

$$[6,2] = r^{2^1} + r^{2^4} + r^{2^7} + r^{2^{10}} + r^{2^{13}} + r^{2^{16}}$$

$$[6, 2] = r^2 + r^3 + r^5 + r^{14} + r^{16} + r^{17}$$

- Pour tout diviseur d de 18, Gauss obtient des *périodes* [d, f], en groupant et ajoutant d racines, à partir de r^f.

- Exemple pour d= 6: on a 3 périodes différentes [6, 1], [6, 2], [6, 4]

j	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

$[6, 2] = r^2+r^3+r^5+r^{14}+r^{16}+r^{17}$ $[6, 1] = r+r^7+r^8+r^{11}+r^{12}+r^{18}$

$[6, 4] = r^4+r^6+r^9+r^{10}+r^{13}+r^{15}$

[6, 1], [6, 2], [6, 4] sont les racines de $x^3+x^2-6x+7=0$

- On continue et on décompose les périodes [6, f] en périodes [2, g]

- Exemple : [6, 1]=[2, 1]+[2, 7]+[2, 8]

$$
\begin{aligned}
[6,\ 1] &= r+r^{7}+r^{8}+r^{11}+r^{12}+r^{18} \\
&= \left(r+r^{18}\right)+\left(r^{7}+r^{12}\right)+\left(r^{8}+r^{11}\right) \\
&= (r^{2^{18}}+r^{2^{9}})+(r^{2^{6}}+r^{2^{15}})+(r^{2^{3}}+r^{2^{12}})
\end{aligned}
$$

- [2, 1], [2, 7], [2, 8] sont les racines de

x^3- [6,1]x^2+ ([6, 1]+[6, 4])x-2-[6,2]=0

- Finalement, toute racine de l'équation initiale est solution d'une équation quadratique à coefficients des fonctions rationnelles de [2,1], [2, 7], etc...

$$
\Omega = (18,1) \ldots\ldots \left\{
\begin{array}{l}
(6,1) \left\{ \begin{array}{l} (2,\ 1) \ldots\ldots [1],\ [18] \\ (2,\ 8) \ldots\ldots [8],\ [11] \\ (2,\ 7) \ldots\ldots [7],\ [12] \end{array} \right. \\[2ex]
(6,2) \left\{ \begin{array}{l} (2,\ 2) \ldots\ldots [2],\ [17] \\ (2,16) \ldots\ldots [3],\ [16] \\ (2,14) \ldots\ldots [5],\ [14] \end{array} \right. \\[2ex]
(6,4) \left\{ \begin{array}{l} (2,\ 4) \ldots\ldots [4],\ [15] \\ (2,13) \ldots\ldots [6],\ [13] \\ (2,\ 9) \ldots\ldots [9],\ [10]. \end{array} \right.
\end{array}
\right.
$$

Division du cercle

- Etude de $(x^p-1)/(x-1)=x^{p-1}+x^{p-2}+\ldots+x+1=0$, p premier >2
- Racines $\zeta^j = \cos 2\pi j/p + i \sin 2\pi j/p$ avec j=1, ...p-1
- Les exposants j peuvent être exprimés comme des puissances d'une racine primitive mod p (=générateur de (Z/pZ)*) => réordonne les racines
- Les nouveaux groupements des racines conduisent à la décomposition graduelle de l'équation en équations de degrés divisant p-1
- Gauss détermine ainsi quels polygones réguliers peuvent être construits à la règle et au compas : le nombre n de côtés doit être 2^k, ou un nombre premier p tel que $p-1=2^k$ (p est un premier de Fermat), ou un produit $2^k p_1 p_2 \ldots p_r$, avec p_i différent premiers de Fermat.

342. Le but de nos recherches, qu'il n'est pas inutile d'annoncer ici en peu de mots, est de décomposer X *graduellement* en un nombre de facteurs de plus en plus grand, et cela de manière à ce que les coefficiens de ces facteurs puissent être déterminés par des équations du degré le plus bas possible, jusqu'à ce que, de cette manière, on parvienne à des facteurs simples, ou aux racines Ω. Nous ferons voir que si l'on décompose le nombre $p-1$ en facteurs entiers quelconques α, β, γ, etc. (pour lesquels on peut prendre les facteurs premiers), X est décomposable en α facteurs du degré $\frac{n-1}{\alpha}$, dont les coefficiens seront déterminés par une équation du degré α; que chacun de ces facteurs est décomposable en β facteurs du degré $\frac{n-1}{\alpha\beta}$, à l'aide d'une équation de degré β, etc. Desorte que ν étant le nombre des facteurs α, β, γ, etc., la recherche des racines Ω est ramenée à la résolution de ν équations des degrés α, β, γ, etc.

For p=17

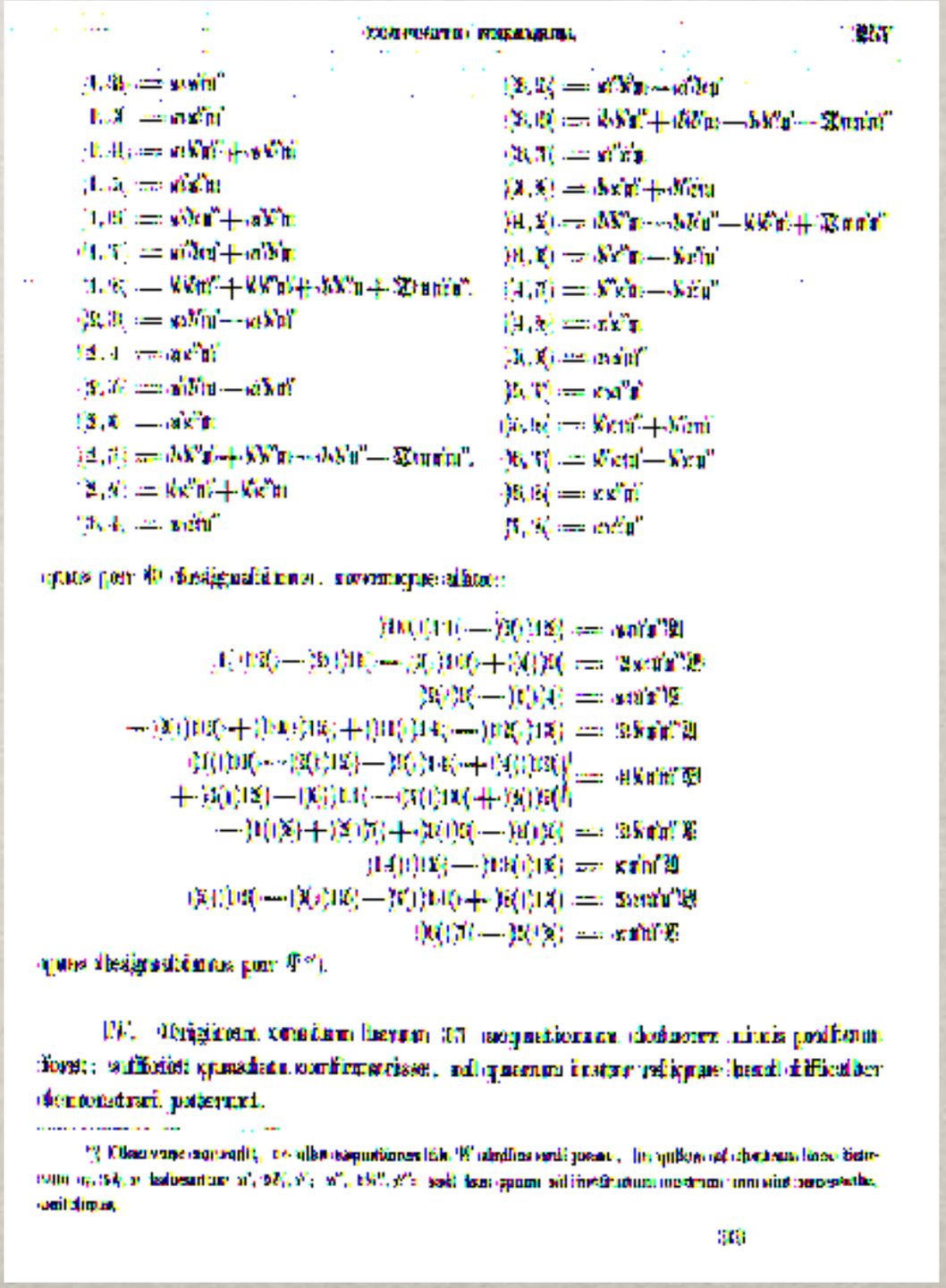
$$\cos\frac{p}{17} = -\tfrac{1}{16} + \tfrac{1}{16}\sqrt{17} + \tfrac{1}{16}\sqrt{(34 - 2\sqrt{17})} - \tfrac{1}{8}\sqrt{\{(17 + 3\sqrt{17}) - \sqrt{(34 - 2\sqrt{17})} - 2\sqrt{(34 + 2\sqrt{17})}\}};$$

Pour résumer

- Nouveaux concepts, nouvelles techniques
- Démonstrations rigoureuses (et parfois très longues)
- Met en lumière équivalence, structures

Pour résumer un peu mieux

- Calculs explicites, effectifs (beaucoup !)
- Importance de la cyclicité
- Complexe organisation systémique de l'ouvrage (et non une organisation linéaire déductive)



[Le système propre aux nouvelles mathématiques] n'est pas seulement un système continu, dont la perfection se trouve uniquement dans le fait que ce qui suit est partout fondé sur ce qui précède, mais un système plus apparenté au système du monde, dont la tâche aujourd'hui doit être d'aller au-delà de la pure fondation de vérités mathématiques et de donner une connaissance globale de leurs relations essentielles les unes aux autres.

E. Kummer, c. 1850

Intermède : effectif-effectif

- 1811-1850 : analyse de l'algorithme d'Euclide pour le calcul du pgcd de 2 entiers
- plus connu : Gabriel Lamé : le nombre de divisions nécessaires est inférieur à 5x nombre de chiffres du plus petit des deux nombres

J. Shallit,
Historia mathematica, 1994

Charles Hermite (1822-1901)

- professeur à l'école Polytechnique, à la Sorbonne, membre de l'Académie des sciences

- théorème d'Hermite-Minkowski sur les minima de formes quadratiques, preuve de la transcendance de *e*, résolution des équations algébriques du 5e degré, théorie de Galois différentielle, …

- *presque:* le théorème des unités de Dirichlet

Lettres à Jacobi, 1847-1850

Hermite considère $f(x_0, x_1 \cdots, x_n)$ une forme quadratique (définie) à $n+1$ variables et à coefficients réels.

$$f(x_0, x_1 \cdots, x_n) = a_{11}x_1^2 + a_{12}x_1x_2 + \cdots + a_{ij}x_ix_j + \cdots + a_{nn}x_n^2$$

Lettre à Jacobi, c. 1847

Hermite considère $f(x_0, x_1 \cdots, x_n)$ une forme quadratique (définie) à $n+1$ variables et à coefficients réels.
Hermite définit le déterminant D de la forme comme celui du système :

$$\frac{1}{2}\frac{df}{dx_0} = X_0,\ \frac{1}{2}\frac{df}{dx_1} = X_1 \cdots,\ \frac{1}{2}\frac{df}{dx_n} = X_n$$

Théorème principal

Il existe $n+1$ entiers α, β, $\cdots$, λ, tels que

$$0 < f(\alpha, \beta, \cdots, \lambda) < \left(\frac{4}{3}\right)^{n/2} \sqrt[n+1]{\mid D \mid}$$

Lettre à Jacobi, c. 1847 : et Gauss?

Théorème principal

Il existe $n+1$ entiers α, β, $\cdots$, λ, tels que

$$0 < f(\alpha, \beta, \cdots, \lambda) < \left(\frac{4}{3}\right)^{n/2} \sqrt[n+1]{\mid D \mid}$$

• Pour $n = 1$, c'est la théorie de la réduction : la forme f est équivalente à une forme g dont le premier coefficient est plus petit que $\frac{2}{3}\sqrt{\mid D \mid}$. Ce premier coefficient est une valeur de g en des entiers (c'est $g(1,0)$), donc par changement de variable, c'est une valeur de f en des entiers.

• Pour $n = 2$, D.A. 272 : une forme quadratique à 3 variables est équivalente à une forme, dont le premier coefficient est plus petit que $\frac{4}{3}\sqrt[3]{D}$.

Lettre à Jacobi, c. 1847 : et Gauss?

Théorème principal

Il existe $n+1$ entiers α, β, $\cdots$, λ, tels que

$$0 < f(\alpha, \beta, \cdots, \lambda) < \left(\frac{4}{3}\right)^{n/2} \sqrt[n+1]{\mid D \mid}$$

• D.A. 278-280 : Gauss montre une relation (compliquée) avec certaines formes quadratiques à trois variables et certaines formes quadratiques à 2 variables. Cette relation, généralisée, est la base de la preuve (par récurrence) d'Hermite pour son théorème principal.

Application: approximation simultanée de nombres réels par des fractions

Soit A, B deux nombres réels et Δ un nombre positif quelconque.
Hermite introduit la forme à 3 variables

$$f = (x' - Ax)^2 + (x'' - Bx)^2 + \frac{x^2}{\Delta}$$

Son déterminant est $1/\Delta$. Le théorème principal dit qu'il existe 3 entiers m, m', m'' tels que

$$0 < (m' - Am)^2 + (m'' - Bm)^2 + \frac{m^2}{\Delta} < \frac{4}{3}\frac{1}{\sqrt[3]{\Delta}}$$

$$0 < (m' - Am)^2 + (m'' - Bm)^2 + \frac{m^2}{\Delta} < \frac{4}{3}\frac{1}{\sqrt[3]{\Delta}}$$

Donc :
$\mid m' - Am \mid < \frac{2}{\sqrt{3}}\frac{1}{\sqrt[6]{\Delta}}$, $\mid m'' - Bm \mid < \frac{2}{\sqrt{3}}\frac{1}{\sqrt[6]{\Delta}}$, $\mid m \mid < \frac{2}{\sqrt{3}}\sqrt[3]{\Delta}$.
Ou encore :

$$\mid \frac{m'}{m} - A \mid < \frac{4}{3m\sqrt{m}}$$

$$\mid \frac{m''}{m} - B \mid < \frac{4}{3m\sqrt{m}}$$

AUTRES APPLICATIONS

- périodes de fonctions complexes
- théorème de Sturm sur la séparation des racines
- étude des nombres algébriques

$\alpha, \beta, \cdots, \lambda$ racines réelles d'une équation algébrique irréductible de degré n.
Hermite leur associe une forme quadratique n-aire définie positive

$$f(x_0, x_1, \cdots, x_{n-1}) = D_0\phi^2(\alpha) + D_1\phi^2(\beta) + \cdots + D_{n-1}\phi^2(\lambda),$$

où $\phi(\alpha) = x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots + \alpha^{n-1} x_{n-1}$, etc.

> Peut-être parviendra-t-on à déduire de là [de l'étude des formes dont les coefficients dépendent des racines d'équations algébriques à coefficients entiers] un système complet de caractères pour chaque espèce de ce genre de quantités […]. On ne peut du moins faire concourir trop d'éléments pour jeter quelque lumière sur cette variété infinie des irrationnelles algébriques, dont les symboles d'extraction des racines ne nous représentent que la plus faible partie.…Quelle tâche immense pour la théorie des nombres et le calcul intégral de pénétrer au milieu d'une telle multiplicité d'êtres de raison en les classant par groupes irréductibles entre eux, de les constituer tous individuellement, par des définitions caractéristiques et élémentaires.
>
> Hermite à Jacobi

Peut-être parviendra-t-on à déduire de là [de l'étude des formes dont les coefficients dépendent des racines d'équations algébriques à coefficients entiers] un système complet de caractères pour chaque espèce de ce genre de quantités […]. On ne peut du moins faire concourir trop d'éléments pour jeter quelque lumière sur cette variété infinie des irrationnelles algébriques, dont les symboles d'extraction des racines ne nous représentent que la plus faible partie. …Quelle tâche immense pour la théorie des nombres et le calcul intégral de pénétrer au milieu d'une telle multiplicité d'êtres de raison en les classant par groupes irréductibles entre eux, de les constituer tous individuellement, par des définitions caractéristiques et élémentaires.

Hermite à Jacobi

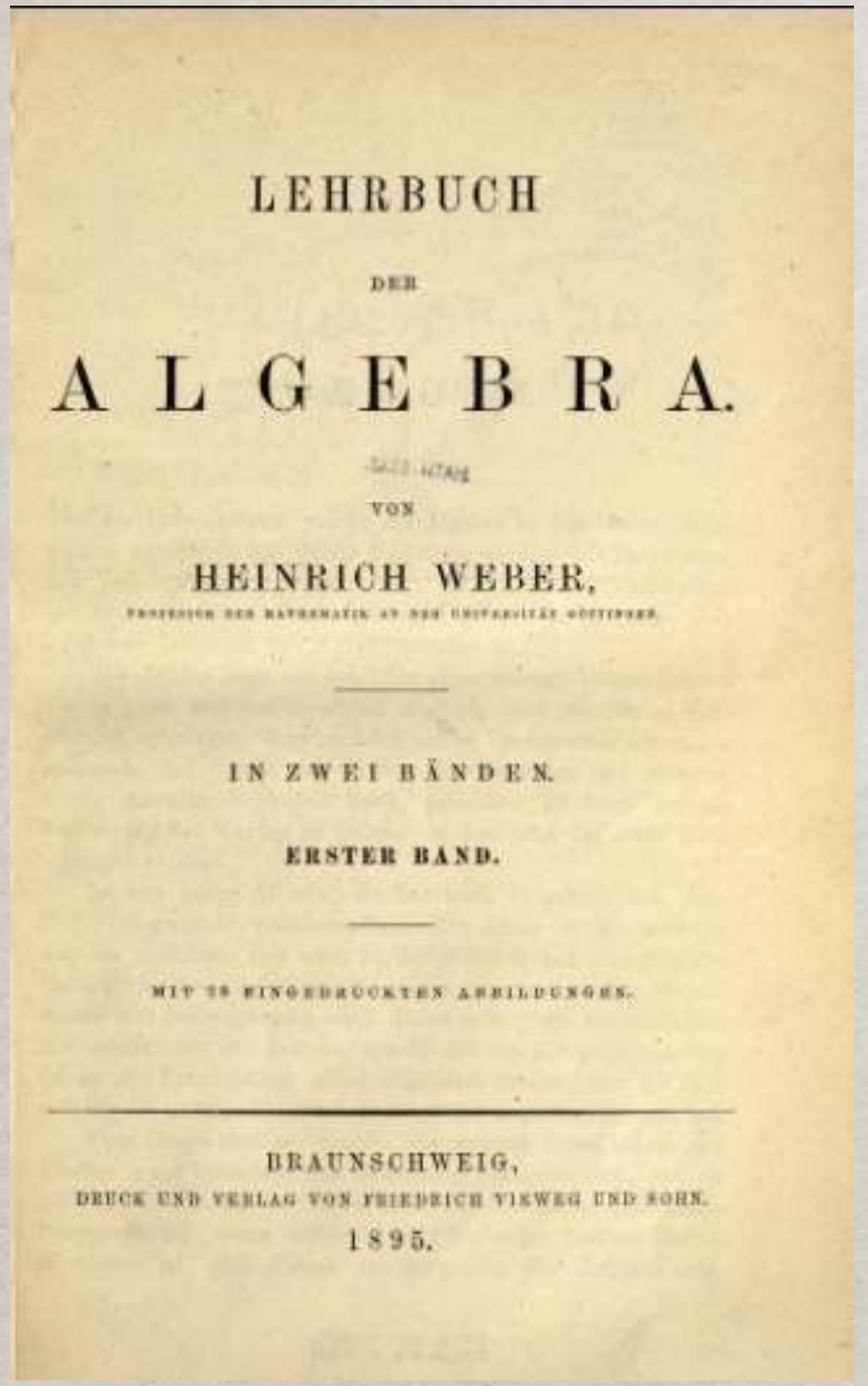
Résolution des équations au 19e siècle

Vos *Disquisitiones* vous ont mis tout de suite au rang des premiers géomètres et je regarde la dernière section comme contenant la plus belle découverte analytique qui ait été faite depuis longtemps. Votre travail sur les planètes aura de plus le mérite de l'importance de son objet.

Lagrange à Gauss, 1804

EQUATIONS ALGEBRIQUES

- 1 modèle : équations du cercle, Gauss DA
- => on cherche des solutions sous la forme de racines successives
- Abel c. 1825 : impossible en général pour degré ≥5 ; résoluble [par radicaux] avec certaines conditions théoriques (ex : toutes les racines s'expriment rationnellement à partir d'une)
- Galois c. 1830 : esquisse d'un programme de décomposition et de conditions de résolubilité


LEHRBUCH

DER

ALGEBRA.

VON

HEINRICH WEBER,

IN ZWEI BÄNDEN.

ERSTER BAND.

MIT 38 EINGEDRUCKTEN ABBILDUNGEN.

BRAUNSCHWEIG,

DRUCK UND VERLAG VON FRIEDRICH VIEWEG UND SOHN.

1895.

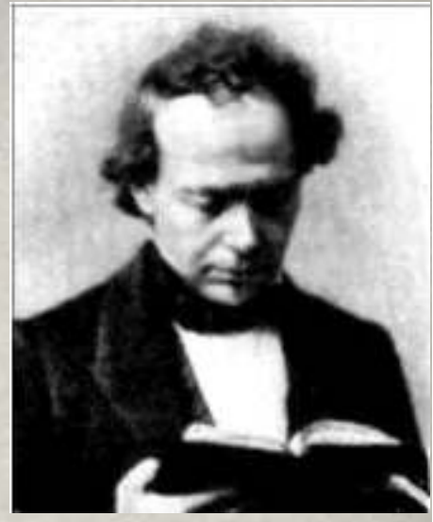
Une des questions les plus anciennes, sur laquelle la nouvelle algèbre a préférentiellement appuyé son développement est de celle de ce qu'on comprend sous le nom de résolution algébrique des équations, soit une représentation des racines d'une équation par une suite de radicaux ou leur calcul par une chaîne finie d'extractions de racines. Sur cette question la lumière la plus claire vient de la théorie des groupes.

Heinrich Weber, *Lehrbuch der Algebra*, vol. 1, p. 592, 1895.

Nature, Formules et calculs explicites

On essaye de distinguer et d'isoler, par certains signes, les différentes racines d'une formule radicale, et cette séparation est tout fait illusoire, car ces racines coexistent toujours dans une seule quelconque d'entre elles; tant qu'on y laisse ces radicaux qui donnent lieu cette multiplicité de valeurs. Or par la nature même de l'Algèbre il faut que ces signes équivoques demeurent, puisque cette science n'a d'autre objet que d'indiquer les opérations à faire, mais sans les exécuter, afin que le tableau de ces opérations, la seule chose que l'esprit ait en vue, soit parfaitement conservé. [...] Lorsqu'on passe aux applications numériques les opérations s'effectuent.

L. Poinsot, Note, in J.-L. Lagrange, *Traité des équations numériques de tous les degrés,* 1826



Je m’attacherai seulement au fait si important annoncé par Galois […] mais on n’arrive ainsi qu’à s’assurer de la possibilité de la réduction, et une lacune importante restait à remplir pour pousser la question jusqu’à son dernier terme.

[…] C’est sous un point de vue bien différent que je vais maintenant traiter les mêmes questions. Laissant de côté toute considération relative aux décompositions de groupe, je définis, a priori, les racines des équations réduites...

$\alpha, \beta, \cdots, \lambda$ racines réelles d'une équation algébrique irréductible de degré n.

Hermite leur associe une forme quadratique n-aire définie positive

$$f(x_0, x_1, \cdots, x_{n-1}) = D_0\phi^2(\alpha) + D_1\phi^2(\beta) + \cdots + D_{n-1}\phi^2(\lambda),$$

où $\phi(\alpha) = x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots + \alpha^{n-1} x_{n-1}$, etc.

> Peut-être parviendra-t-on à déduire de là [de l'étude des formes dont les coefficients dépendent des racines d'équations algébriques à coefficients entiers] un système complet de caractères pour chaque espèce de ce genre de quantités […]. On ne peut du moins faire concourir trop d'éléments pour jeter quelque lumière sur cette variété infinie des irrationnelles algébriques, dont les symboles d'extraction des racines ne nous représentent que la plus faible partie.…Quelle tâche immense pour la théorie des nombres et le calcul intégral de pénétrer au milieu d'une telle multiplicité d'êtres de raison en les classant par groupes irréductibles entre eux, de les constituer tous individuellement, par des définitions caractéristiques et élémentaires.
>
> Hermite à Jacobi

Théorème de Sturm

- Sturm 1829 : Le nombre de racines réelles d'un polynôme compris entre deux bornes a et b est donné par la différence des nombres de changements de signes dans la suite des valeurs en a et b d'une suite explicite de polynômes.

- $V(x) \Rightarrow V_1(x) = V'(x) \Rightarrow V_2(x)$, etc… $V_n(x)$

- On calcule les signes des $V_i(a)$: nombre de changements l

- On calcule les signes des $V_i(b)$: nombre de changements m

- Le nombre de racines réelles distinctes de V entre a et b est m-l

- Construction de Sturm de la suite V_i : divisions euclidiennes

- c. 1840 : J. Sylvester donne une expression a priori explicite des V_i en fonction des racines de V, a_i

Théorème de Sturm

$$\frac{V_1}{V} = \sum \frac{1}{x - a_i}$$

$$\frac{V_2}{V} = \sum \frac{(a_i - a_j)^2}{(x - a_i)(x - a_j)}$$

$$\frac{V_3}{V} = \sum \frac{(a_i - a_j)^2 (a_i - a_k)^2 (a_j - a_k)^2}{(x - a_i)(x - a_j)(x - a_k)}$$

$$\vdots$$

$$\frac{V_m}{V} = \frac{\prod_{i \neq j} (a_i - a_j)^2}{\prod_i (x - a_i)}$$

Hermite sur Sturm

Soit $\Delta_{i,t}$ les déterminants correspondant aux formes :

$$\sum \frac{x_0^2}{t-a_i}, \sum \frac{(x_0+a_i x_1)^2}{t-a_i}, \sum \frac{(x_0+a_i x_1+a_i^2 x_2)^2}{t-a_i}, \text{ etc.}$$

$$\Delta_{m-1,t} = \frac{1}{\prod(x-a_i)} \begin{vmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{m-1} \\ 1 & a_2 & a_2^2 & \dots & a_1^{m-1} \\ \vdots & \vdots & & \ddots & \vdots \\ 1 & a_m & a_m^2 & \dots & a_m^{m-1}. \end{vmatrix}$$

La forme f_t se réduit par une transformation linéaire réelle à :

$$f_t = \Delta_0 X_0^2 + \frac{\Delta_1}{\Delta_0} X_1^2 + \frac{\Delta_2}{\Delta_1} X_2^2 + \ldots + \frac{\Delta_{m-1}}{\Delta_{m-2}} X_{m-1}^2.$$

Réciproquement, le théorème de Sturm se lit sur les signatures de f_a, f_b
Extension aux racines complexes, à plusieurs équations, etc.

Hermite sur la résolution des équations algébriques

Cette impossibilité [de résoudre par radicaux les équations de degré supérieur ou égal au 5e] manifeste en effet la nécessité d'introduire quelque élément analytique nouveau dans la recherche de la solution…Au lieu de chercher à représenter par une formule radicale à déterminations multiples le système des racines si étroitement liées entre elles lorsqu'on les considère comme fonctions des coefficients, on peut ... chercher, en introduisant des variables auxiliaires, à obtenir les racines séparément exprimées par autant de fonctions distinctes et uniformes relatives à ces nouvelles variables.

Équations

Cette impossibilité [de résoudre par radicaux les équations de degré supérieur ou égal au 5e] manifeste en effet la nécessité d'introduire quelque élément analytique nouveau dans la recherche de la solution…Au lieu de **chercher à représenter par une formule radicale à déterminations multiples le système des racines si étroitement liées entre elles lorsqu'on les considère comme fonctions des coefficients,** on peut ... chercher, en introduisant des variables auxiliaires, à obtenir les racines séparément exprimées par autant de fonctions distinctes et uniformes relatives à ces nouvelles variables.

$$x^3 - 3x + 2a = 0$$

$$x = \epsilon \sqrt[3]{\sqrt{a^2 - 1} - a} - \epsilon^2 \sqrt[3]{\sqrt{a^2 - 1} + a}, \qquad \epsilon^3 = 1$$

Équations

Cette impossibilité [de résoudre par radicaux les équations de degré supérieur ou égal au 5e] manifeste en effet la nécessité d'introduire quelque élément analytique nouveau dans la recherche de la solution…Au lieu de chercher à représenter par une formule radicale à déterminations multiples le système des racines si étroitement liées entre elles lorsqu'on les considère comme fonctions des coefficients, on peut ... **chercher, en introduisant des variables auxiliaires, à obtenir les racines séparément exprimées par autant de fonctions distinctes et uniformes relatives à ces nouvelles variables.**

$$x^3 - 3x + 2a = 0$$

$$2\sin\frac{\alpha}{3}, 2\sin\frac{\alpha+2\pi}{3}, 2\sin\frac{\alpha+4\pi}{3}$$

Hermite sur l'équation modulaire

Je m'attacherai seulement au fait si important annoncé par Galois et qui consiste en ce qu[e les équations modulaires] sont susceptibles d'un abaissement au degré inférieur d'une unité dans les cas de n = 5, n=7 et n=11. ... Il n'est pas difficile en suivant la voie qu'il a ouverte de retrouver la démonstration de cette belle proposition; mais on n'arrive ainsi qu'à s'assurer de la possibilité de la réduction, et une lacune importante restait à remplir pour pousser la question jusqu'à son dernier terme.

[…] C'est sous un point de vue bien différent [de celui de M. Betti] que je vais maintenant traiter les mêmes questions. Laissant de côté toute considération relative aux décompositions de groupe, je définis, a priori, les racines des équations réduites...

Équations modulaires

Fonctions elliptiques de Jacobi

$$y = F(k, \Theta) = \int_0^{\Theta} \frac{d\theta}{\sqrt{1 - k^2 sin\theta}}, \qquad 0 < k < 1$$

$$y = \int_0^{sn(y,k)} \frac{1}{\sqrt{(1-x^2)(1-k^2x^2)}} dx$$

k module, *k'*=√*(1-k²)* module complémentaire, Θ amplitude, *sn =sin am*

$$K = \int_0^1 \frac{1}{\sqrt{(1-x^2)(1-k^2x^2)}} dx$$

(Demi)-Périodes *K* et *iK'*

$$K' = \int_0^1 \frac{1}{\sqrt{(1-x^2)(1-k'^2x^2)}} dx$$

$$q = e^{-\pi \frac{K'}{K}} = e^{i\pi\omega}$$

Équations modulaires

$$q = e^{-\pi \frac{K'}{K}} = e^{i\pi\omega}$$

$$\sqrt[4]{k} =: \phi(\omega), \qquad \sqrt[4]{k'} =: \psi(\omega)$$

$$\sqrt[4]{k}\left(\frac{a\omega + b}{c\omega + d}\right) =: \phi\left(\frac{a\omega + b}{c\omega + d}\right) = (-1)^{\frac{a^2+ab-1}{8}} \sqrt[4]{k}(\omega)$$

Pour n premier, le polynôme de degré n+1

$$P_n(x,k) = \left[x - \left(\frac{2}{n}\right) \sqrt[4]{k(n\omega)}\right] \prod_{0 \le m < n} \left[x - \sqrt[4]{k\left(\frac{\omega + 16m}{n}\right)}\right]$$

a des coefficients polynômes rationnels en $\phi(\omega)$

Équations modulaires

Autrement dit, il existe une relation algébrique («équation modulaire ») de degré n+1 entre

$$u = \sqrt[4]{k(\omega)} =: \phi(\omega) \qquad \text{et} \qquad v = \sqrt[4]{k(n\omega)}$$

Exemple, pour n=5 :

$$u^6 - v^6 + 5u^2v^2(u^2 - v^2) + 4uv(1 - u^4v^4) = 0$$

Hermite sur l'équation modulaire

$$\Phi(\omega) = \left[\phi(5\omega) + \phi(\frac{\omega}{5})\right]\left[\phi(\frac{\omega+16}{5}) - \phi(\frac{\omega+4.16}{5})\right]\left[\phi(\frac{\omega+2.16}{5}) - \phi(\frac{\omega+3.16}{5})\right]$$

Alors, $\Phi(\omega), \Phi(\omega+16), \Phi(\omega+2.16), \Phi(\omega+3.16), \Phi(\omega+4.16)$

sont les 5 racines d'une équation de degré 5, à coefficients rationnels en $\phi(\omega)$

$$\Phi^5 - 2^4 5^3 \Phi \phi^4(\omega)\psi^{16}(\omega) - 2^6\sqrt{5^5}\phi^3(\omega)\psi^{16}(\omega)[1+\phi^8(\omega)] = 0$$

Hermite sur l'équation quintique

$$\Phi^5 - 2^4 5^3 \Phi \phi^4(\omega)\psi^{16}(\omega) - 2^6\sqrt{5^5}\phi^3(\omega)\psi^{16}(\omega)[1+\phi^8(\omega)] = 0$$

Réciproquement, en partant de l'équation du 5e degré de Jerrard

$$x^5 - x - a = 0 \qquad *$$

En posant :

$$a = \frac{2}{\sqrt[4]{5}^5}\frac{1+\phi^8(\omega)}{\phi^2(\omega)\psi^4(\omega)}$$

on tire k, ω, et la résolution de l'équation quintique * par les fonctions elliptiques « en tant que les racines se trouvent représentées séparément par des fonctions uniformes »

Hermite sur les équations algébriques

Ces premières propriétés d'irrationnelles algébriques, non exprimables par radicaux, me paraissent du plus grand intérêt; comme les propriétés des racines des équations relatives à la division du cercle, elles serviront de point de départ pour pénétrer plus avant dans la théorie générale des équations.

Hermite à Jacobi, c. 1848

Leopold Kronecker

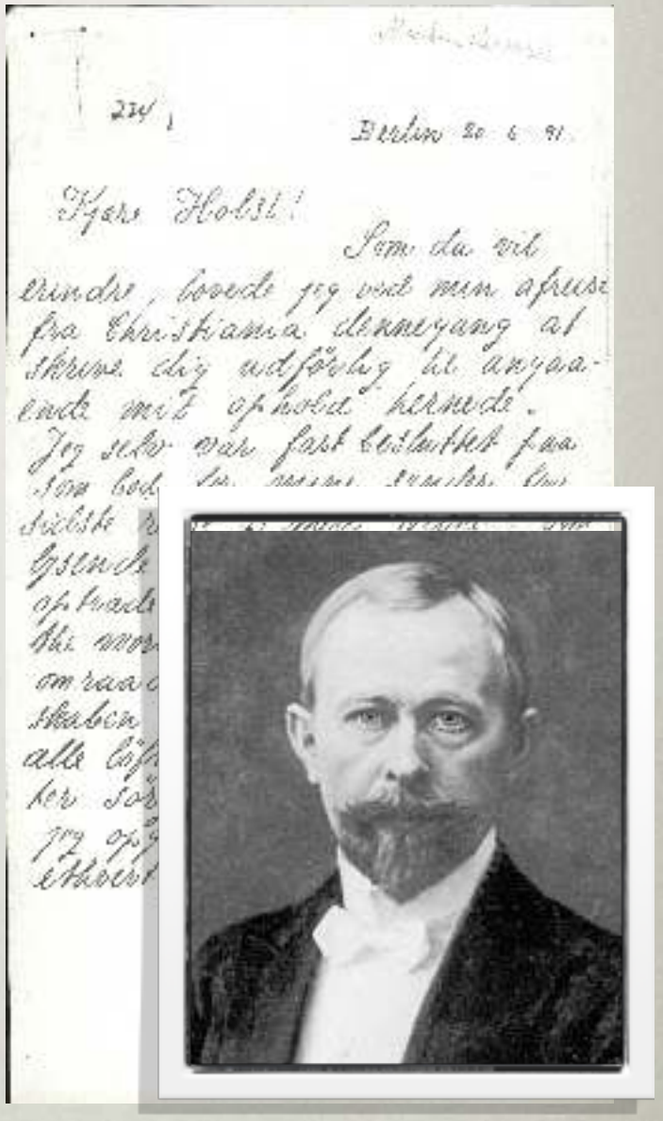
- Naissance en 1823, lycée à Liegnitz où Ernst Kummer est professeur.
- 1841-1845 : Etudes universitaires à Berlin, Bonn, Breslau
- 1845 : thèse (dir. Dirichlet) sur les unités complexes
- 1845-1855 : affaires familiales
- 1853… : retourne aux mathématiques (à titre privé) à Berlin
- 1861: élection à l'Académie de Berlin (et correspondant à celle de Göttingen), autorisé à donner des cours à l'université
- 1881 : coréd. du Journal für die reine und angewandte Mathematik
- 1883 : reprend chaire de Kummer à Berlin

7/12/1823 - 29/12/1891

Axel Thue a Berlin (1890-1891)

Palmstrøm et moi avons assisté au cours de Kronecker sur la théorie des équations algébriques. Il est remarquable pour sa grande profondeur et sa rigueur minutieuse, mais il a la mauvaise habitude lorsqu'il est pris par son enthousiasme de donner les définitions et d'autres informations absolument essentielles bien trop rapidement. […] C'est un homme extrêmement sympathique, mais il préfère faire la conversation lui-même, et longuement.

Thue à Holst, 20 juin 1891



Les cours de Kronecker

L'Auditorium 17, c'est une sombre pièce ; j'ai rêvé sous son ombre maint rêve pesant.
E. Pringsheim, cité par A. Kneser, 1925

L'ensemble du cours est un mélange superficiel confus d'idées non digérées, de vantardise, de divagations non motivées et de blagues paresseuses.
G. Cantor, cité par H. Edwards, *Essays in Constructive Mathematics*, 2005

Kronecker aimait commencer par une introduction bien arrangée, entremêlée de phrases acérées et spirituelles, qui pouvaient atteindre les oreilles de tous les auditeurs et qui donnaient à chacun l'illusion agréable qu'il comprenait quelque chose. Mais cela passait. Rapidement, l'orateur se précipitait dans les secrets d'une science en train de naître, avec lesquels, comme il se plaisait à le dire, il n'avait commencé à lutter que la nuit précédente.
A. Kneser, 1925

L’algèbre n’est pas vraiment une discipline en soi, mais un fondement et un outil pour l’ensemble des mathématiques, et son développement rapide dans les dernières années a été en fait suscité et dirigé par les besoins d’autres disciplines mathématiques.

L. Kronecker, Discours d’entrée à l’Académie de Berlin, 1861

Leopold Kronecker

- unités complexes, cyclotomie
- “groupes” abéliens (2 définitions différentes…)
- fonctions elliptiques et modulaires, équation quintique
- système de périodes de fonctions complexes, approximation par des rationnels
- théorème de Sturm
- théorie des invariants, formes bilinéaires, diviseurs élémentaires
- théorie arithmétique des grandeurs algébriques

7/12/1823 - 29/12/1891

Une vraie valeur scientifique, dans le champ des mathématiques, je la reconnais seulement dans des vérités mathématiques concrètes, ou pour le dire plus précisément, “seulement dans des formules mathématiques”. Celles-ci seules, comme le montre l’histoire des mathématiques, sont impérissables. Les différentes théories sur les fondements des mathématiques (comme celle de Lagrange) ont été balayées par le temps, mais la résolvante de Lagrange est restée.

Leopold Kronecker à Georg Cantor, 21 août 1884

Avec l'introduction de principe des indéterminées (*indeterminatae*), qui dérive de Gauss, la théorie particulière des nombres entiers s'est étendue à la théorie arithmétique générale des fonctions entières d'indéterminées, à coefficients entiers. Cette théorie générale permet de se séparer de tous les concepts étrangers à l'arithmétique proprement dite, ceux des nombres négatifs, fractionnaires, algébriques réels et complexes.

Le concept de nombre négatif peut être évité en remplaçant dans les formules le facteur -1 par une indéterminée x et le signe d'égalité par le signe de congruence de Gauss *modulo* $(x+1)$.
Ainsi l'égalité 7-9 =3-5 sera transformée en la congruence
$7+9x \equiv 3-5x$ modulo $(x+1)$. Elle y gagne aussi un contenu, étant donné que la congruence a un sens pour tout entier x positif […] et d'autre part, cette congruence se convertit directement en une égalité […] dans laquelle on introduit à la place de l'indéterminée x l'unité négative.

L. Kronecker, "Über den Zahlbegriff" [Sur le concept de nombre], *Journal für die reine und angewandte Mathematik*, 1887

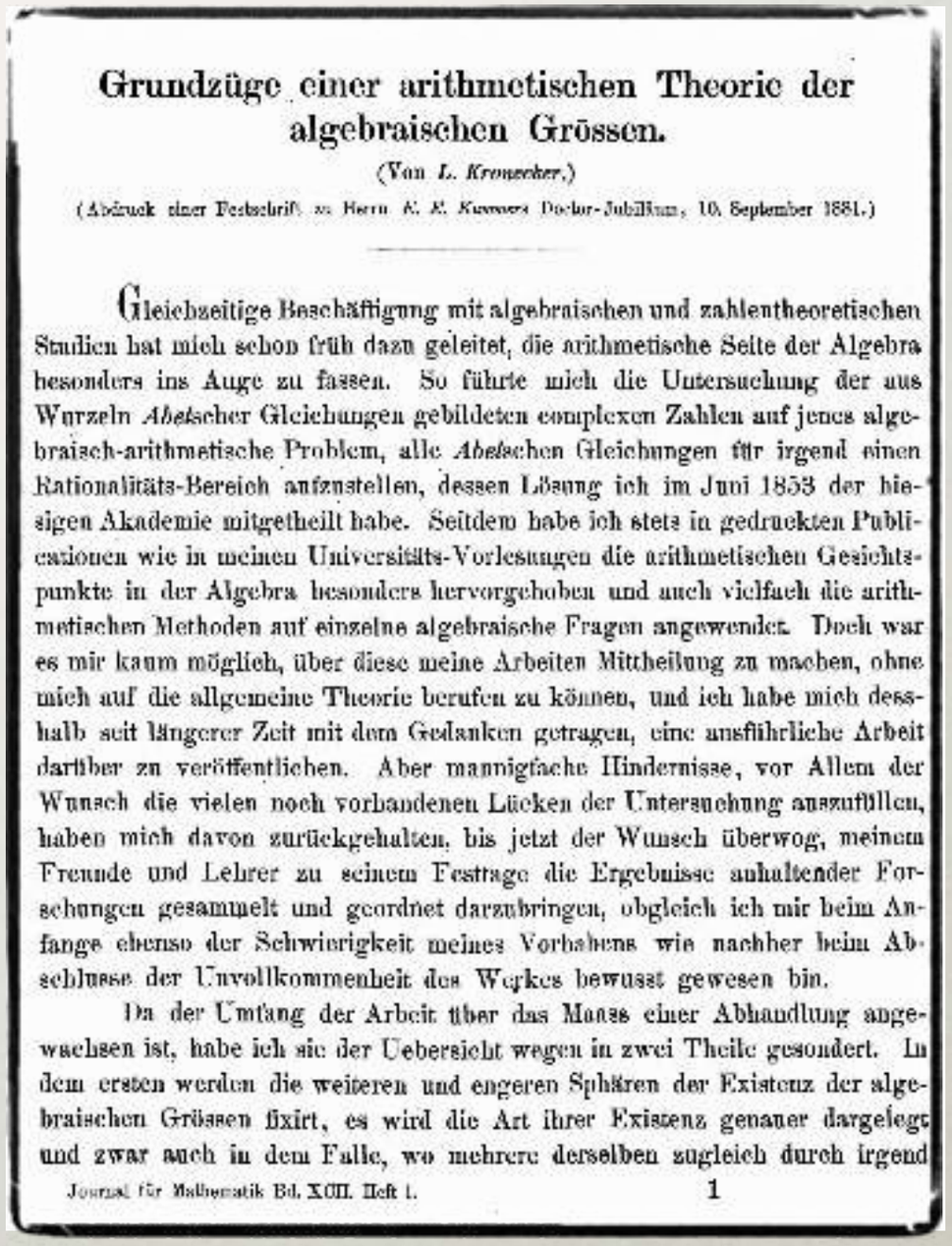
Les définitions devront être algébriques et non pas logiques seulement.

Il ne suffit pas de dire : Une chose est ou elle n'est pas. Il faut montrer ce que veut dire être et ne pas être, dans le domaine particulier dans lequel nous nous mouvons. Alors seulement nous faisons un pas en avant. Si nous définissons, par exemple, une fonction irréductible comme une fonction qui n'est pas réductible, c'est-à-dire qui n'est pas décomposable en d'autres fonctions d'une nature déterminée, nous ne donnons point de définition algébrique, nous n'énonçons qu'une simple vérité logique. Pour *qu'en algèbre,* nous soyons en droit de donner cette définition, il faut qu'elle soit précédée de l'exposé d'une méthode nous permettant d'obtenir à l'aide d'un nombre fini d'opérations rationnelles, les facteurs d'une fonction réductible. Seule cette méthode donne aux mots *réductible* et *irréductible* un sens algébrique.

J. Molk, "Sur une notion qui comprend celle de divisibilité et sur la théorie générale de l'élimination", *Acta mathematica*, 1885

théorie arithmétique des grandeurs algébriques

- 200 pages du journal…
- essentiellement programmatique !
- beaucoup d'appels à ses cours…
- autour d'algorithmes et d'objets abstraits de ses travaux précédents et futurs
- groupe : extrinsèque à la question, fonction entière : intrinsèque, concret



Grundzüge einer arithmetischen Theorie der algebraischen Grössen.

(Von *L. Kronecker.*)

(Abdruck einer Festschrift zu Herrn *E. E. Kummers* Doctor-Jubiläum, 10. September 1881.)

Gleichzeitige Beschäftigung mit algebraischen und zahlentheoretischen Studien hat mich schon früh dazu geleitet, die arithmetische Seite der Algebra besonders ins Auge zu fassen. So führte mich die Untersuchung der aus Wurzeln *Abel*scher Gleichungen gebildeten complexen Zahlen auf jenes algebraisch-arithmetische Problem, alle *Abel*schen Gleichungen für irgend einen Rationalitäts-Bereich aufzustellen, dessen Lösung ich im Juni 1853 der hiesigen Akademie mitgetheilt habe. Seitdem habe ich stets in gedruckten Publicationen wie in meinen Universitäts-Vorlesungen die arithmetischen Gesichtspunkte in der Algebra besonders hervorgehoben und auch vielfach die arithmetischen Methoden auf einzelne algebraische Fragen angewendet. Doch war es mir kaum möglich, über diese meine Arbeiten Mittheilung zu machen, ohne mich auf die allgemeine Theorie berufen zu können, und ich habe mich desshalb seit längerer Zeit mit dem Gedanken getragen, eine ausführliche Arbeit darüber zu veröffentlichen. Aber mannigfache Hindernisse, vor Allem der Wunsch die vielen noch vorhandenen Lücken der Untersuchung auszufüllen, haben mich davon zurückgehalten, bis jetzt der Wunsch überwog, meinem Freunde und Lehrer zu seinem Festtage die Ergebnisse anhaltender Forschungen gesammelt und geordnet darzubringen, obgleich ich mir beim Anfange ebenso der Schwierigkeit meines Vorhabens wie nachher beim Abschlusse der Unvollkommenheit des Werkes bewusst gewesen bin.

Da der Umfang der Arbeit über das Maass einer Abhandlung angewachsen ist, habe ich sie der Uebersicht wegen in zwei Theile gesondert. In dem ersten werden die weiteren und engeren Sphären der Existenz der algebraischen Grössen fixirt, es wird die Art ihrer Existenz genauer dargelegt und zwar auch in dem Falle, wo mehrere derselben zugleich durch irgend

Journal für Mathematik Bd. XCII. Heft 1. 1

Cf exposé de F. Brechenmacher, IHP 2014, en ligne

- 1ère partie : domaines d'existence des grandeurs algébriques
  - domaines sources (Stammbereich) : rationnels, ajout d'indéterminées en nombre fini
  - domaines de genre (Gattungsbereich) : ajout (en nombre fini) de grandeurs vérifiant des équations algébriques
  - algorithme pour tester irréductibilité
  - entiers définissant des espèces dans un genre, discriminant, théorie générale de l'élimination
  - "théorie de Galois" : déterminer les équations d'une certaine classe (même affect) pour un domaine de rationalité donné.
- 2ème partie : arithmétique des espèces : division, pgcd, etc.
  - divisibilité défini par des congruences modulo des fonctions rationnelles ("système de modules" ou "diviseur")
  - interprétation géométrique (intersection de courbes, décomposition en composantes irréductibles)

Décomposition d'une fonction entière

• Kronecker veut une procédure (finie) pour trouver les diviseurs d'une fonction entière à coefficients entiers d'un certain nombre d'indéterminées sur le domaine de rationalité naturel.

• Cas à une indéterminée : $F(x)$ de degré $2n$ ou $2n+1$. Il s'agit de chercher les diviseurs $f(x)$ de degré au plus n.

Kronecker utilise la formule d'interpolation de Lagrange. On choisit $r_0, \ldots, r_n$, $n+1$ entiers arbitraires.

$$f(x) = \sum_k f(r_k) \frac{\prod_{i \neq k}(x - r_i)}{\prod_{i \neq k}(r_k - r_i)}.$$

Décomposition d'une fonction entière

On choisit $r_0, \ldots, r_n$ $n+1$ entiers arbitraires.

$$f(x) = \sum_k f(r_k) \frac{\prod_{i \neq k}(x - r_i)}{\prod_{i \neq k}(r_k - r_i)}.$$

Si $f(x)$ est un facteur de $F(x)$, alors $f(r)$ divise $F(r)$ pour tous les $r = r_k$.

Il y a un nombre fini de possibilités de $f(r_k)$ et donc un nombre fini de $f(x)$ possibles à tester.

Décomposition d'une fonction entière

• Cas à plusieurs indéterminées : $F(x', x'', x''', ...)$.
Kronecker pose $x' = x$, $x'' = x^g$, $x''' = x^{g^2}$, ...
Il choisit g assez grand pour que toues les termes aient des degrés différents
($g >$ max (degrés par rapport à chaque indéterminée)).

Une décomposition de F donne une décomposition de la fonction à une indéterminée $F(x, x^g, x^{g^2}, \ldots)$.
Il y a donc un nombre fini de possibilités à tester pour cette fonction. De même pour la fonction de départ.

Décomposition d'une fonction entière

• Cas à plusieurs indéterminées : $F(x', x'', x''', ...)$.
Kronecker donne aussi une autre méthode, qui procède par récurrence.
Il isole une indéterminée, x', et choisit encore des entiers r_i et des polynômes $g_i(x)$ qui s'annulent pour $x = r_k, k \neq i$ et valent 1 en r_i.
On cherche ensuite les diviseurs de $F(x', x'', x''', ...)$ sous la forme

$$b_0 g_0(x') + b_1 g_1(x') + \cdots ,$$

,
où les b_i sont des fonctions entières à $m - 1$ indéterminées $x'', x''', \ldots$.
Les b_i doivent diviser $F(r_i, x'', x''', \ldots)$.
Par l'hypothèse de récurrence, ceci se teste en un nombre fini de possibilités.

Décomposition d'une fonction entière

On choisit $r_0, \ldots, r_n$ $n+1$ entiers arbitraires.

$$f(x) = \sum_k f(r_k) \frac{\prod_{i \neq k}(x - r_i)}{\prod_{i \neq k}(r_k - r_i)}.$$

Si $f(x)$ est un facteur de $F(x)$, alors $f(r)$ divise $F(r)$ pour tous les $r = r_k$.

Il y a un nombre fini de possibilités de $f(r_k)$ et donc un nombre fini de $f(x)$ possibles à tester. Mais parfois beaucoup !
Dans ses cours, Kronecker remarque seulement qu'on peut se réduire à ceux qui donnent une fonction $f(x)$ entière.

Cas d'un domaine de genre

Soit α vérifiant une équation algébrique à coefficients entiers.
On s'intéresse à la décomposition d'une fonction entière $f(z)$ sur $\mathbb{Q}(z_1, z_2, \ldots, z_n, \alpha)$.
Kronecker pose $x = y - u\alpha$, avec u une nouvelle indéterminée.
La fonction entière $\prod f(y - u\alpha^\sigma)$ (avec α^σ les conjugués de α) est à coefficients dans $\mathbb{Q}(z_1, z_2, \ldots, z_n)$, donc se factorise en un nombre fini de facteurs f_i.
Les pgcd des f_i et de $f(y - u\alpha)$ donnent les facteurs de $f(y - u\alpha)$, donc finalement ceux de $f(x)$.

$$4(x^3 - a^3) \equiv (x - a)(2x + z + a)(2x - z + a) \mod z^2 + 3a^2$$

Pb fondamental : écrire une fonction entière de x comme produit de facteurs linéaires sans définir préalablement les grandeurs algébriques

L. Kronecker, “Ein Fundamental Satz der allgemeinen Arithmetik” [Un théorème fondamental de l’arithmétique générale], *Journal für die reine und angewandte Mathematik*, 1887

Carl Runge

- 1876-1880 : Etudes à université de Munich (avec Max Planck), puis à Berlin
- 1880 : thèse avec Weierstrass, puis cercle de Kronecker
- 1886 : professeur à université de Hanovre, se consacre à la physique, en particulier à la spectroscopie.
- c. 1900 : approximation et convergence, Runge-Kutta
- 1904 : professeur de mathématiques appliquées (le premier poste de ce genre en Allemagne) à l'université de Göttingen, à l'initiative de Planck, Klein, etc.

Décomposition pratique d'une fonction entière : Runge 1886

Runge s'appuie sur deux faits :
• Si f(x) est à coefficients entiers, $\frac{f(x)-f(r_k)}{x-r_k}$ est une fonction entière à coefficients entiers :
$f(r_i) - f(r_k)$ est divisible par $r_i - r_k$.
• Soit a_0 le coefficient du terme de plus haut degré de F, a_p le coefficient du terme constant. Des estimations simples montrent que, avec ρ un majorant des racines de F, on doit avoir, pour un diviseur f de degré au plus m :

$$\mid f(r_i) \mid < \mid a_0 \mid (\mid r_i \mid + \rho)^m - \mid a_0 \mid \rho^m + \mid a_p \mid$$

et

$$\mid f(r_i) \mid > \frac{\mid F(r_i) \mid}{\mid a_0 \mid (\mid r_i \mid + \rho)^{p-m} - \mid a_0 \mid \rho^{p-m} + \mid a_p \mid}.$$

Décomposition pratique d'une fonction entière : Runge 1886

Procédure : On choisit les r_i en maximisant leurs différences, mais en restant dans les tables de factorisation. On trouve dans ces tables les diviseurs θ_0 de $F(r_0)$. On fait une liste. On exclut ceux qui sont hors bornes.
On ne garde parmi les diviseurs θ_1 de $F(r_1)$ que ceux tels que $\theta_1 \equiv \theta_0 \mod r_1 - r_0$, pour un θ_0 de la liste. On les inclut dans un tableau. On exclut ceux qui sont hors bornes.
De même, on ne garde parmi les diviseurs θ_2 de $F(r_2)$ que ceux tels que $\theta_2 \equiv \theta_0 \mod r_2 - r_0$ et $\theta_2 \equiv \theta_1 \mod r_2 - r_1$, pour un θ_0 et un θ_1 du tableau. On les inclut dans le tableau. On exclut ceux qui sont hors bornes. Etc.

Décomposition pratique d'une fonction entière : Runge 1886

On fabrique avec le même procédé les valeurs possibles de $f_1(x) = \dfrac{f(x) - f(r_0)}{r - r_0}$, pour $x = r_1, r_2, ...$, la condition étant que

$$f_1(r_i) \equiv f_1(r_k) \mod r_i - r_k.$$

On itère.
Finalement, on obtient l'expression de $f(x)$:

$$f(x) = f(r_0) + f_1(r_1)(x - r_0) + f_2(r_2)(x - r_0)(x - r_1) + \cdots \\ + f_n(x - r_0)(x - r_1)\ldots(x - r_{n-1}).$$

Décomposition pratique d'une fonction entière : Runge 1886

Runge donne l'exemple :

$$F(x) = 3x^7 + 7x^6 - 10x^5 - 19x^4 + 172x^3 + 71x^2 + 17x - 66.$$

$\varrho = 5$

	$\pm F(x)$	$A^{(1)}$	$B^{(1)}$	$A^{(2)}$	$B^{(2)}$	$A^{(3)}$	$B^{(3)}$
7	17.293.631	0,	36	4,	432	44,	4900
0	2.3.11	0,	15	0,	66	0,	66
—2	$2^3.139$	0,	21	0,	138	0,	720
—8	$2.7.19.127^2$	0,	39	4,	498	44,	6300

Décomposition pratique d'une fonction entière : Runge 1886

$F(x) = 3x^7 + 7x^6 - 10x^5 - 19x^4 + 172x^3 + 71x^2 + 17x - 66.$
Runge choisit $r_0 = 7$, $r_1 = -8$, $r_2 = 0$, $r_3 = -2$.
Le procédé lui donne $f(x) = 1$, $f(x) = x - 6$ (qui n'est pas possible), $x^3 + 5x^2 + 7x - 6$.

Finalement :
$F(x) = (x^3 + 5x^2 + 7x - 6)(3x^4 - 8x^3 + 9x^2 + 10x + 11).$

		$m=1$		$m=2$		$m=3$					
	7	1		17		293				631	
$f(x)$	−8	1	−14	2	−133	−7	−127	38	1778	−254	
	0	1	−6	66	3			6	−22	−6	
	−2	1	−8	8	−1			−4	−4	−8	−278
$f_1(x)$	−8	0	1	1	10			17	−99	59	
	0	0	1	−7	2			41	45	91	
	−2	0	1	1	~~2~~			~~33~~	33	71	101
$f_2(x)$	0	0	0	−1					18	4	
	−2	0	0	Ø					22	2	~~7~~
f_3		0	0						−~~2~~	1	

"Il serait utile [...] d'avoir des procédés rationnels, des formules faciles à retenir, qui permissent d'exécuter, sans hésitation ni perte de temps, la mise en carte du satin proposé. La plupart du temps, lorsque l'on a de semblables dispositions de satins à écrire, on procède par de longs tâtonnements". (Édouard Gand, *Bulletin de la Société industrielle d'Amiens*, 1867)

=> **Edouard Lucas** c. 1870-1880: Arithmétique des restes mod n (arithmétique modulaire, des résidus, des congruences…) appliquée aux problèmes textiles

Edouard Lucas (1842-1891)

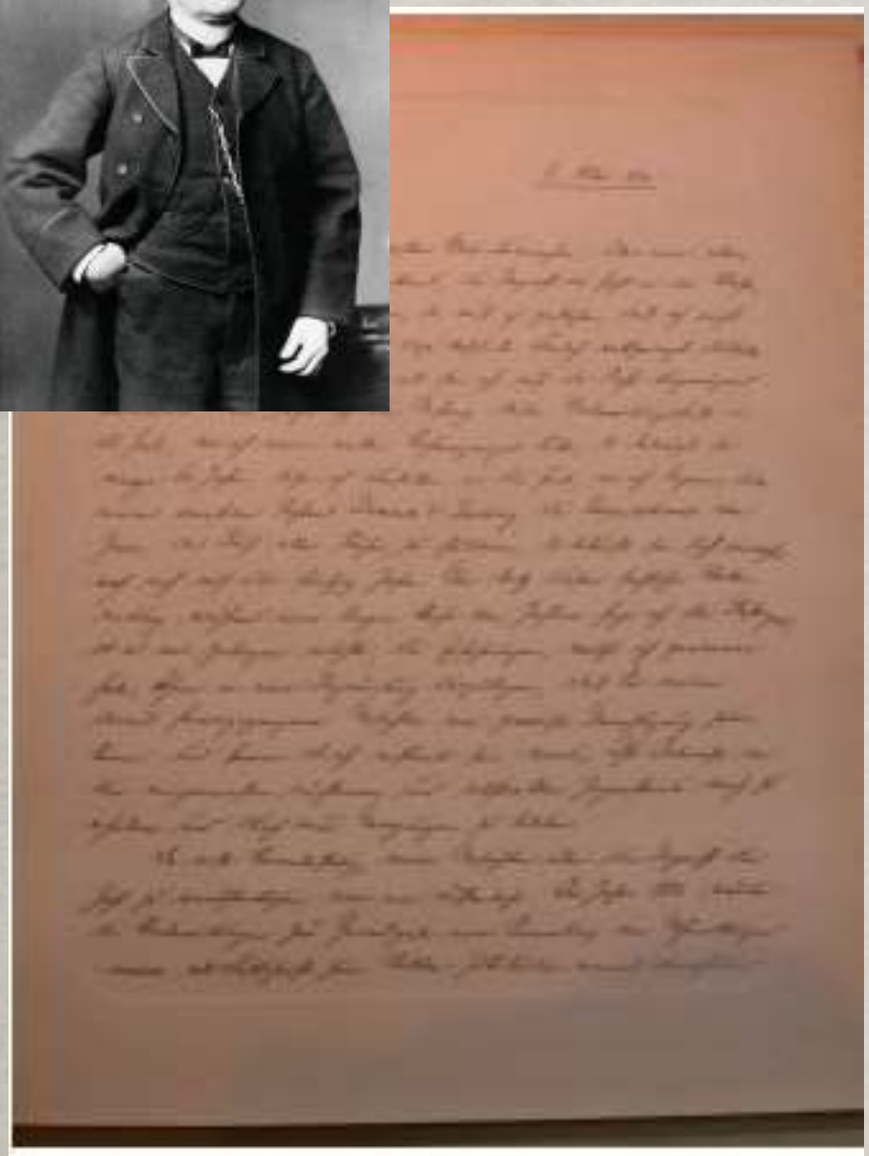
DE LA NATURE ...

L'étude des fonctions de l'analyse est aussi l'étude des lois de nature ; je crois pour mon compte que tous les faits analytiques existent en dehors de nous et s'imposent tout aussi nécessairement que les propriétés de la matière et les phénomènes du monde réel. Par conséquent, je vois dans l'étude des fonctions une étude de la réalité objective, et dans les lois relatives aux fonctions, un reflet des lois physiques.
Hermite à Paul du Bois-Reymond, 1er février 1881

Je renonce à vous développer […] mon objectif […] de faire une science d'observation des connaissances les plus abstraites en rapprochant (je n'ose dire plus) les mathématiques et la théorie des fonctions des sciences naturelles, en voyant dans les nombres premiers, les irrationnelles, les transcendantes, des réalités en dehors de nous qui s'imposent avec la même nécessité que les substances et tous les êtres de la nature visible.
Hermite à Paul du Bois-Reymond, 3 septembre 1887

[Mon propre travail] illustrerait de manière très frappante à quel point l'observation, la divination, l'induction, la procédure expérimentale, et la vérification, la causalité également (si ceci signifie, comme je le suppose, aller des phénomènes à leurs raisons ou causes d'être), sont pertinentes pour le travail du mathématicien.

James Joseph Sylvester, British Association for the Advancement of Science, 1869.



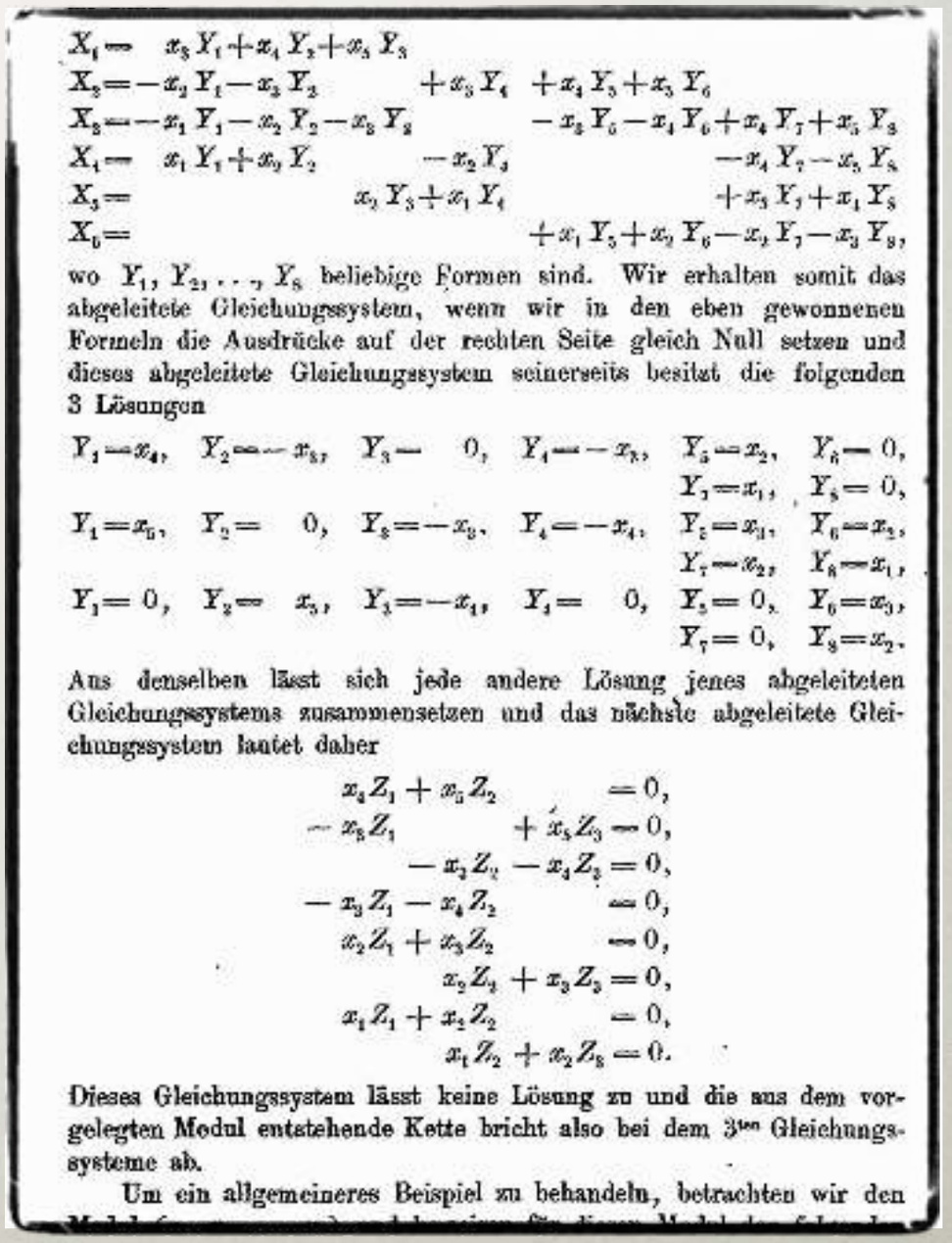
Manuscrit du cours de L. Kronecker
conservé à la bibliothèque de l'IRMA, Strasbourg

La mathématique n'est rien d'autre qu'une science naturelle et ce qui lui importe donc aussi, c'est de "décrire simplement et complètement les phénomènes". Les définitions des sciences empiriques, c'est-à-dire des mathématiques et des sciences de la nature […] ne doivent pas seulement être non contradictoires, mais elles doivent être puisées dans l'expérience. Et, ce qui est encore plus essentiel, elles doivent comporter en elles-mêmes le critère selon lequel on peut décider, dans chaque cas particulier, si la notion donnée est, ou non, à subsumer sous cette définition.

L. Kronecker, *Sur le concept de nombre*, cours Berlin 1891 (éd. J. Boniface et N. Schappacher, RHM 7 (2001), 207-275)

HERITAGE DE KRONECKER

- Très important !
- Pas seulement l'opposition "épistémologique" à Dedekind et Cantor
- Voir Encyclopédie de Klein-Meyer
- Voir Hilbert !



$$
\begin{aligned}
X_1 &= x_3 Y_1 + x_4 Y_2 + x_5 Y_3 \\
X_2 &= -x_2 Y_1 - x_3 Y_2 + x_5 Y_4 + x_4 Y_5 + x_5 Y_6 \\
X_3 &= -x_1 Y_1 - x_2 Y_2 - x_3 Y_3 - x_3 Y_5 - x_4 Y_6 + x_4 Y_7 + x_5 Y_8 \\
X_4 &= x_1 Y_1 + x_2 Y_2 - x_2 Y_3 - x_4 Y_7 - x_5 Y_8 \\
X_5 &= x_2 Y_3 + x_1 Y_4 + x_5 Y_7 + x_4 Y_8 \\
X_6 &= + x_1 Y_5 + x_2 Y_6 - x_2 Y_7 - x_3 Y_8,
\end{aligned}
$$

wo $Y_1, Y_2, \ldots, Y_8$ beliebige Formen sind. Wir erhalten somit das abgeleitete Gleichungssystem, wenn wir in den eben gewonnenen Formeln die Ausdrücke auf der rechten Seite gleich Null setzen und dieses abgeleitete Gleichungssystem seinerseits besitzt die folgenden 3 Lösungen

$$
\begin{array}{llllll}
Y_1 = x_4, & Y_2 = -x_3, & Y_3 = 0, & Y_4 = -x_3, & Y_5 = x_2, & Y_6 = 0, \\
 & & & & Y_7 = x_1, & Y_8 = 0, \\
Y_1 = x_5, & Y_2 = 0, & Y_3 = -x_3, & Y_4 = -x_4, & Y_5 = x_1, & Y_6 = x_2, \\
 & & & & Y_7 = x_2, & Y_8 = x_1, \\
Y_1 = 0, & Y_2 = x_5, & Y_3 = -x_4, & Y_4 = 0, & Y_5 = 0, & Y_6 = x_3, \\
 & & & & Y_7 = 0, & Y_8 = x_2.
\end{array}
$$

Aus denselben lässt sich jede andere Lösung jenes abgeleiteten Gleichungssystems zusammensetzen und das nächste abgeleitete Gleichungssystem lautet daher

$$
\begin{aligned}
x_4 Z_1 + x_5 Z_2 &= 0, \\
-x_3 Z_1 + x_5 Z_3 &= 0, \\
-x_2 Z_2 - x_4 Z_3 &= 0, \\
-x_3 Z_1 - x_4 Z_2 &= 0, \\
x_2 Z_1 + x_3 Z_2 &= 0, \\
x_2 Z_2 + x_3 Z_3 &= 0, \\
x_1 Z_1 + x_2 Z_2 &= 0, \\
x_1 Z_2 + x_2 Z_3 &= 0.
\end{aligned}
$$

Dieses Gleichungssystem lässt keine Lösung zu und die aus dem vorgelegten Modul entstehende Kette bricht also bei dem 3ten Gleichungssysteme ab.

Um ein allgemeineres Beispiel zu behandeln, betrachten wir den

Grete Hermann

- 1876-1880 : Etudes à université de Göttingen
- 1926 : thèse dir. Emmy Noether, mais se tourne finalement vers la philosophie
- 1927 : assistante de Leonard Nelson
- 1927- 1934 : collaboration avec Minna Specht (cofondatrice de l'Internationaler Sozialistischer Kampfbund) pour l'édition posthume de l'oeuvre de Nelson et s'engage contre la montée du nazisme
- 1934-7 : séjour à Leipzig (Heisenberg) et au Danemark, s'intéresse aux fondements de la quantique, prix Ac. sci. Leipzig.
- 1937: se réfugie en Angleterre, "mariage"
- 1946 - 1966 : Pädagogische Hochschule de Bremen (professeur titulaire en 1950)

1901 - 1984

Thèse

- “La question du nombre fini de pas dans la théorie des idéaux de polynômes”, publié dans les *Mathematischen Annalen* en 1926
- origine : travail de K. Hentzelt, mort à la guerre, travail revisité par E. Noether (qui reformule de manière structurale et théorique)

Die Frage der endlich vielen Schritte in der Theorie der Polynomideale.

(Unter Benutzung nachgelassener Sätze von K. Hentzelt.)

Von

Grete Hermann in Göttingen.

Die Ringbereiche, in denen die in der vorliegenden Arbeit auftretenden Ideale definiert sind, sollen Polynombereiche sein. Ein Ideal soll *gegeben* heißen, wenn eine *Basis* des Ideals bekannt ist, es heißt *berechenbar*, wenn sich eine *Basis* berechnen läßt. In dieser Arbeit soll es sich darum handeln, die für ein gegebenes Ideal $\mathfrak{m}$ charakteristischen Ideale und Polynome zu berechnen. Die Berechnung stützt sich dabei auf die Ideal- und Eliminationstheorie, wie sie von E. Noether und K. Hentzelt entwickelt ist [1]). Für die benutzten Grundbegriffe verweise ich insbesondere auf die Zusammenstellung N. § 1. Einige Änderungen in den Definitionen und weitere Zusätze werden in § 1 dieser Arbeit gegeben.

Die folgenden Rechenmethoden werden Berechnungen mit *endlich vielen Schritten* sein. Die Behauptung, eine Berechnung kann mit endlich vielen Schritten durchgeführt werden, soll dabei bedeuten, es kann eine *obere Schranke für die Anzahl der zur Berechnung notwendigen Operationen* angegeben werden. Es genügt also z. B. nicht, ein Verfahren anzugeben, von dem man theoretisch nachweisen kann, daß es mit endlich vielen Operationen zum Ziele führt, wenn für die Anzahl dieser Operationen keine obere Schranke bekannt ist [2]). Die in der vorliegenden Arbeit

[1]) E. Noether, Idealtheorie in Ringbereichen, Math. Annalen **83** (1921), S. 24–66. K. Hentzelt, Zur Theorie der Polynomideale u. Resultanten, bearbeitet von E. Noether, Math. Annalen **88** (1922), S. 53–79, zitiert H. N. E. Noether, Eliminationstheorie und allgemeine Idealtheorie, Math. Annalen **90** (1923), S. 229–261, zitiert N. Für die benutzten Begriffe der Körpertheorie sei verwiesen auf E. Steinitz, Algebraische Theorie der Körper, Journal für Mathematik **137** (1910), S. 167–309, zitiert St.

[2]) Macaulay, der im Anschluß an die Laskersche Arbeit [Zur Theorie der Moduln und Ideale, Math. Annalen **60**] Wege zur Berechnung der zu einem Ideal

Thèse

- “Les méthodes de calcul qui suivent sont des calculs à un nombre fini de pas. [Ceci] doit signifier qu’on peut donner une borne supérieure pour le nombre des opérations nécessaires au calcul. Il n’est donc pas suffisant de donner une procédure dont on peut démontrer qu’elle s’effectuerait en un nombre fini d’opérations, si aucune borne supérieure n’est donnée pour le nombre d’opérations”.
- Objectif : calculer avec des idéaux de polynômes.

Calcul du ppcm de deux idéaux donnés

Lemme : Soit $f_{ij}(x_1, x_2, \ldots, x_n)$ dans $\mathbb{Q}(x_1, x_2, \ldots, x_n)$.
Il est possible de trouver en un nombre fini d'opérations une solution complète [i. e. un ensemble de solutions dont toute solution se déduit par combinaison linéaire à coefficients dans $\mathbb{Q}(x_1, x_2, \ldots, x_n)$] aux équations :

$$\begin{array}{c} f_{11}z_1 + f_{12}z_2 + \cdots f_{1s}z_s = 0 \\ \cdots \\ f_{t1}z_1 + f_{12}z_2 + \cdots f_{ts}z_s = 0 \end{array}$$

Soit q= sup (deg f_{ij}). Le degré des polynômes de la solution est inférieur à $\sum_{i=0}^{n}(qt)^{2^i}$.

Calcul du ppcm de deux idéaux donnés

Soit deux idéaux $A = (f_1, \ldots, f_t)$ et $B = (g_1, \ldots, g_s)$. Un élément c est dans le ppcm de A et B s'il s'écrit $c = d_1 f_1 + \cdots + d_t f_t = e_1 g_1 + \cdots + e_s g_s$.

Hermann applique le lemme à l'équation :
$d_1 f_1 + \cdots + d_t f_t - e_1 g_1 - \cdots - e_s g_s = 0$.

Elle obtient une "solution complète" en un nombre fini d'opérations :

$$d_{11}, \ldots, d_{1t}, e_{11}, \ldots, e_{1s}$$

$$\ldots\ldots\ldots$$

$$d_{k1}, \ldots, d_{kt}, e_{k1}, \ldots, e_{ks}$$

Calcul du ppcm de deux idéaux donnés

Donc

$$c_1 = d_{11}f_1 + \cdots + d_{1t}f_t = e_{11}g_1 + \cdots + e_{1s}g_s$$
$$\cdots\cdots$$
$$c_k = d_{k1}f_1 + \cdots + d_{kt}f_t = e_{k1}g_1 + \cdots + e_{ks}g_s$$

est une base du ppcm de A et B.

Division d'un idéal par un autre

De même, soit les formes linéaires (à coefficients polynomiaux)

$$l_1 = f_{11}z_1 + f_{12}z_2 + \cdots f_{1s}z_s$$
$$\cdots\cdots\cdots$$
$$l_t = f_{t1}z_1 + f_{12}z_2 + \cdots f_{ts}z_s$$

Un élément l du module engendré par ces formes l_i est tel que $l = a_1 l_1 + \cdots + a_t l_t$.

On peut choisir cette représentation telle que :
$deg(a_i) \leq deg(l) + \sum_{i=0}^{n} (qt)^{2^i}$.

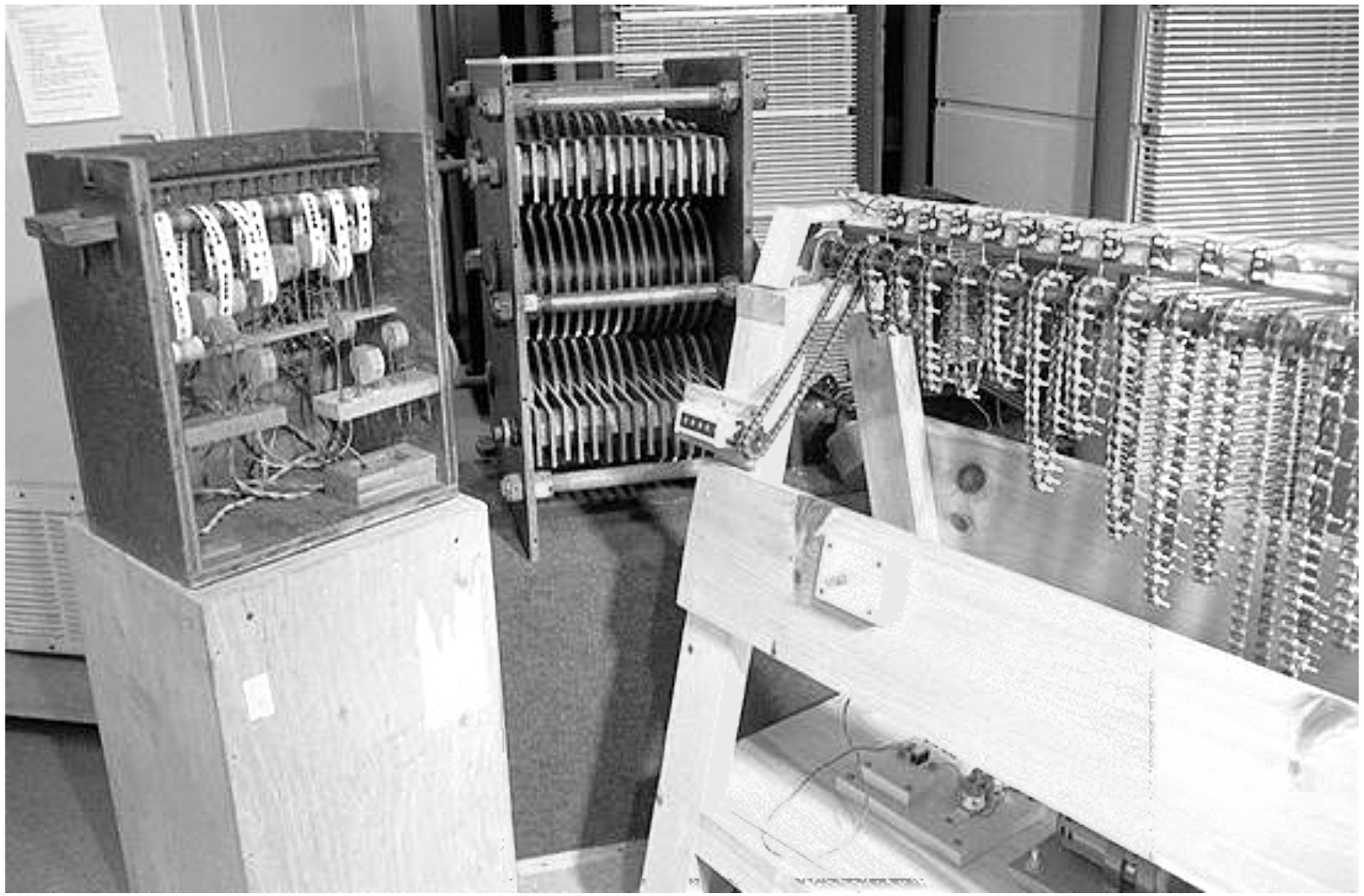
Corollaire : critère (en un nombre fini d'opérations) pour décider si un idéal divise un autre.

Votre thèse était déjà si abstraite et formelle. Etant donné cela, vous devriez choisir un sujet avec un contenu important. Autrement, vous seriez en danger d'être seulement capable de déduire et plus de juger de manière autonome.

L. Nelson to Hermann, cité par Inge Hansen-Schaberg, *A Biographical Sketch*… 2017

Implémentation

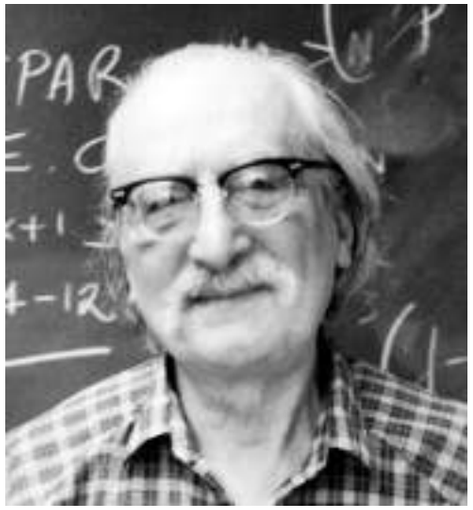
- Exclusion : cribles
- Machines à cribler : baguettes, cellules photo-électriques et chaînes de vélo



Les cribles de D. H. Lehmer (c. 1930)

Algorithme Baby Step Giant Step

(d'après *Handbook of Applied Cryptography*)



- Origine : Daniel Shanks (CLASNO)… et la section V des Recherches arithmétiques de Gauss !
- Question : G groupe cyclique = <a> à n éléments et x dans G, donc $x=a^g$. Calculer g.
- (1): Soit $m=E(\sqrt{n})$, on liste $(j,\ a^j)$ pour $0\leq j\leq m$ et on ordonne selon la 2e composante
- (2) Si x listé, ok, sinon, on teste $x(a^{-m})$, $x(a^{-m})^2$, …
- ordre de grandeur : $C\sqrt{n}$ multiplication dans G

- Tension arithmétique/algèbre/analyse du point de vue de l’effectivité
- Effectivité ou précision ?
- Mathématiques comme sciences naturelles vs mathématiques “instrumentales”
- Quel milieu mathématique pour les analyses d’algorithmes ?

Merci !