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

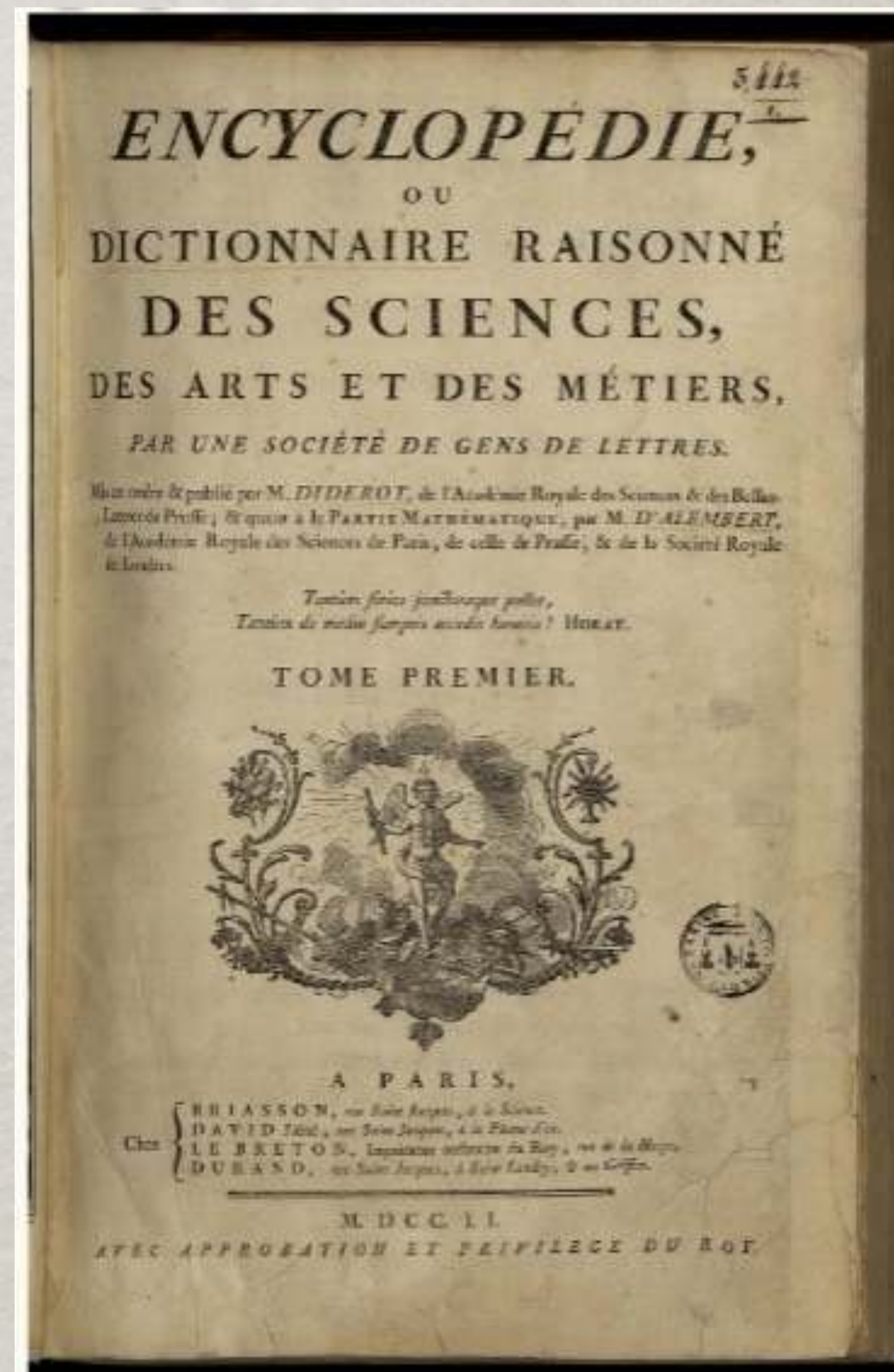
Quelques problèmes

- 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*]



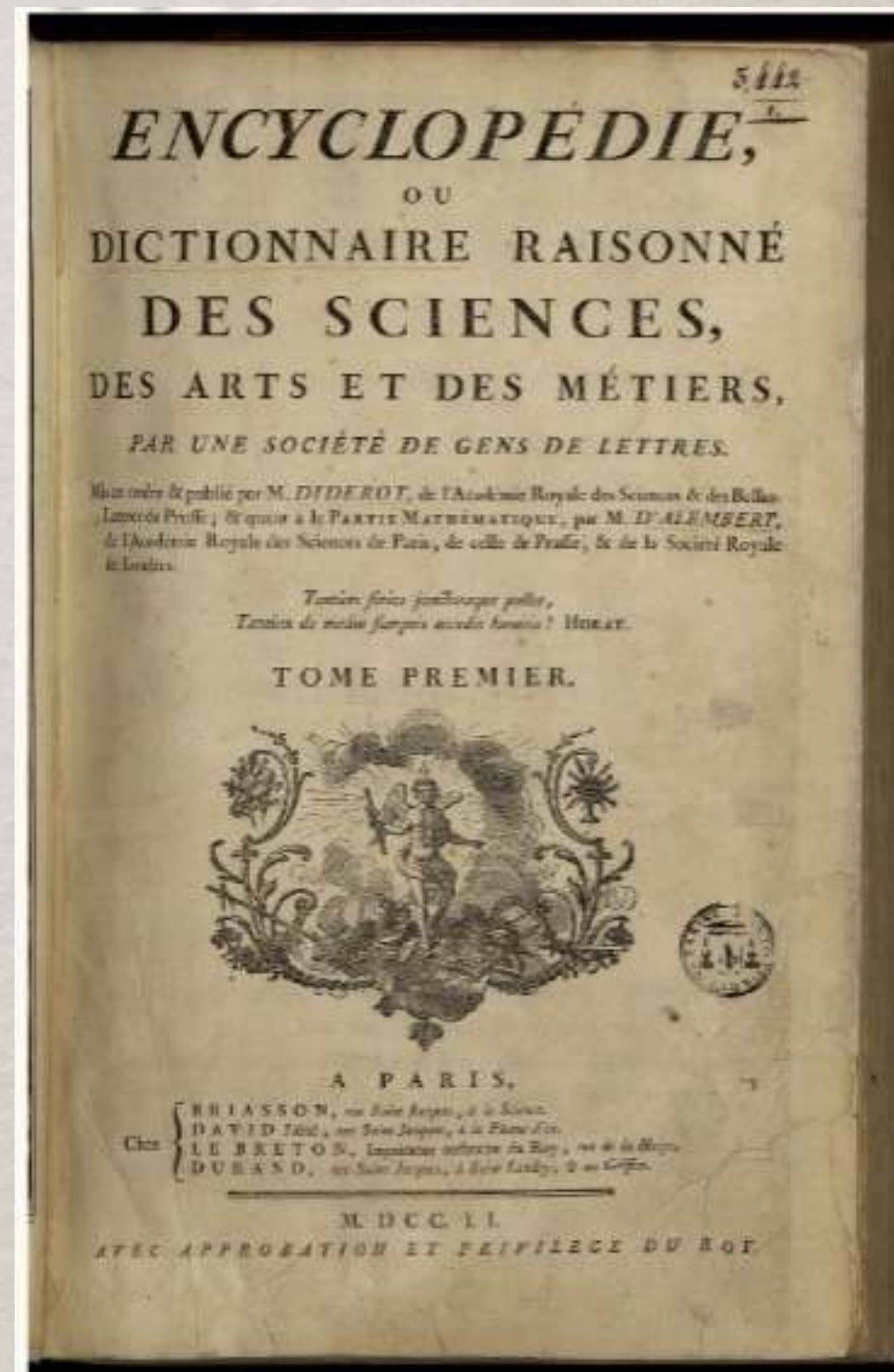
http://enccre.academie-sciences.fr/

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*]



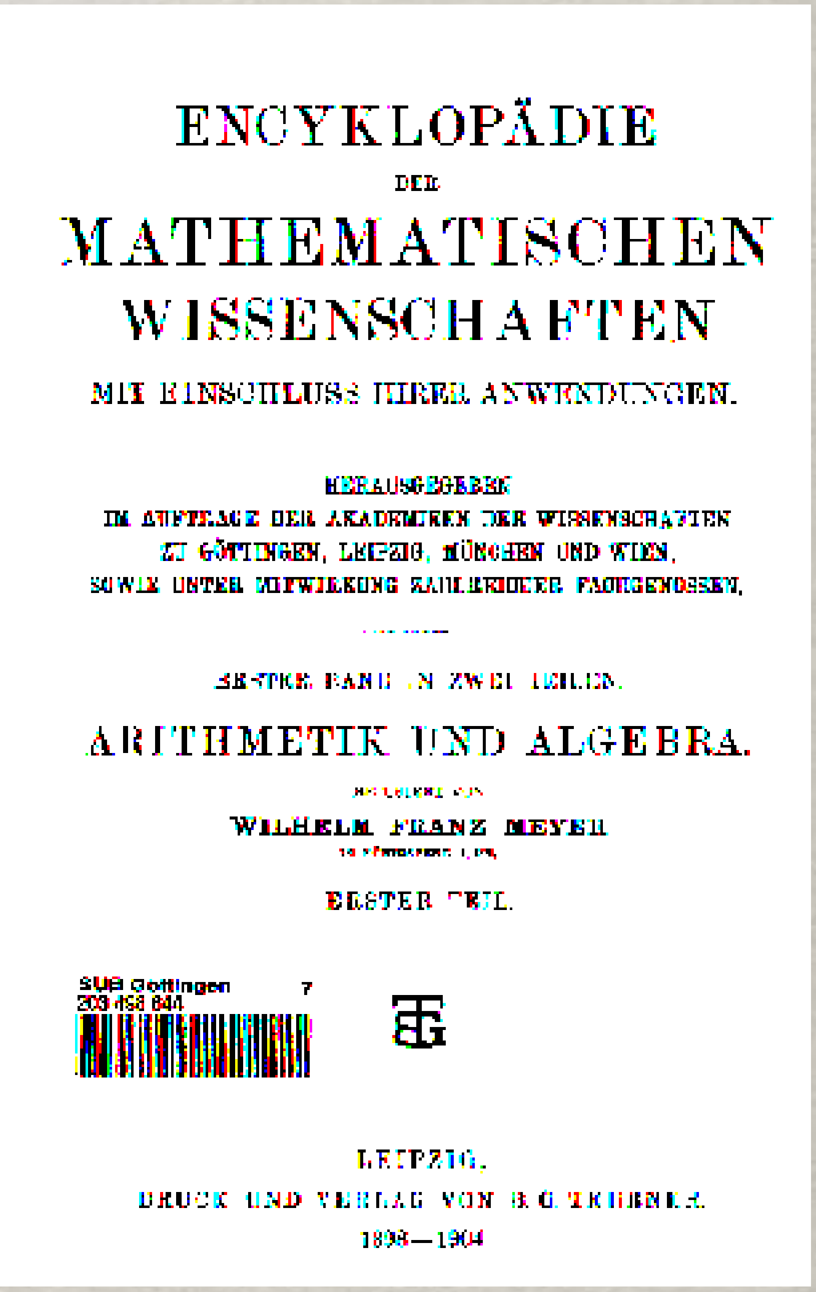
http://enccre.academie-sciences.fr/

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 AKADEMIEEN DER WISSENSCHAFTEN
ZU GÖTTINGEN, LEIPZIG, MÜNCHEN UND WIEN,
SOWIE UNTER MITWIRKUNG ZAHLREICHER FACHGENOSSEN.

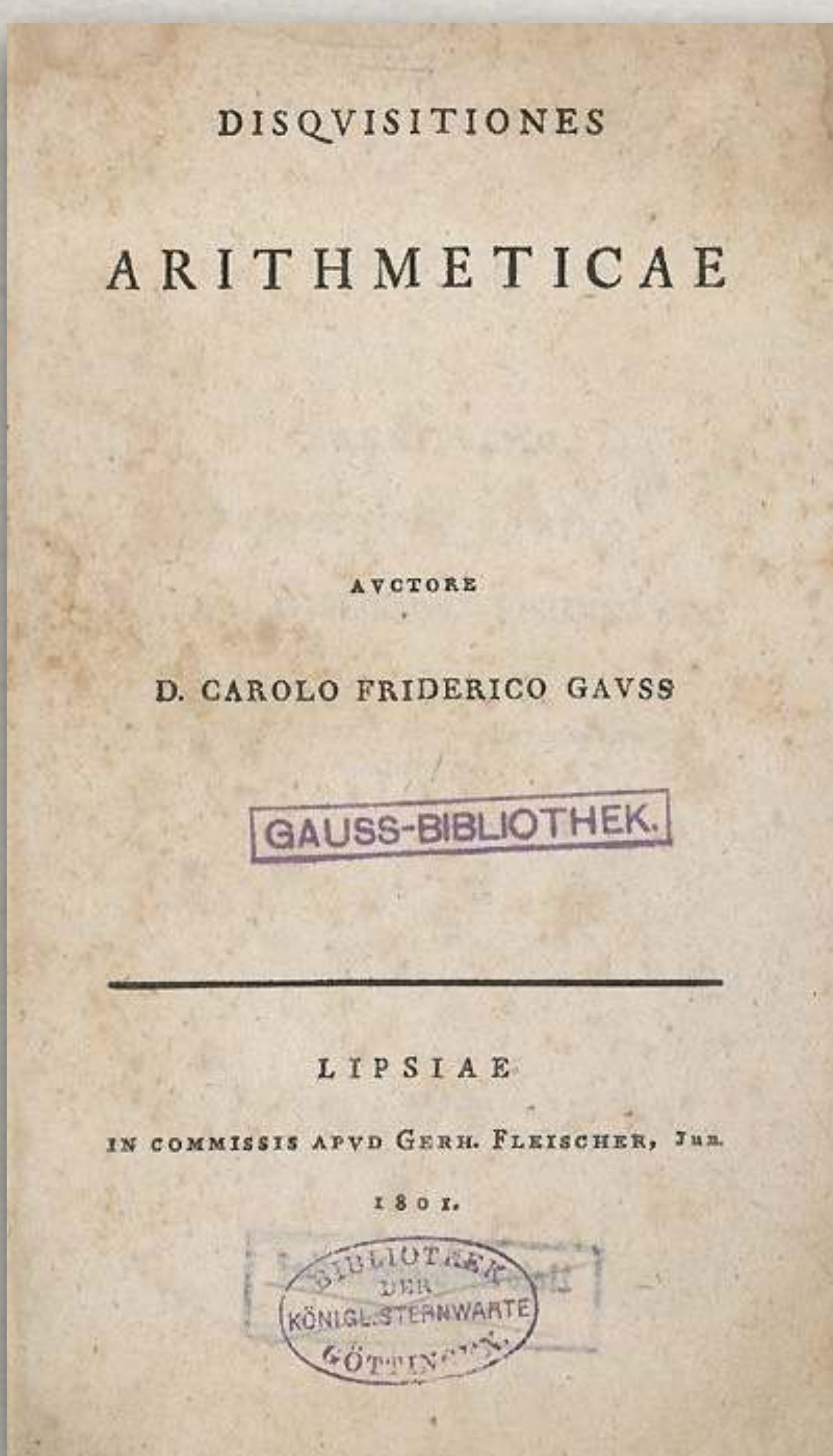
ERSTER BAND IN ZWEI TEILEN.
ARITHMETIK UND ALGEBRA.
WILHELM FRANZ MEYER
ERSTER TEIL.

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

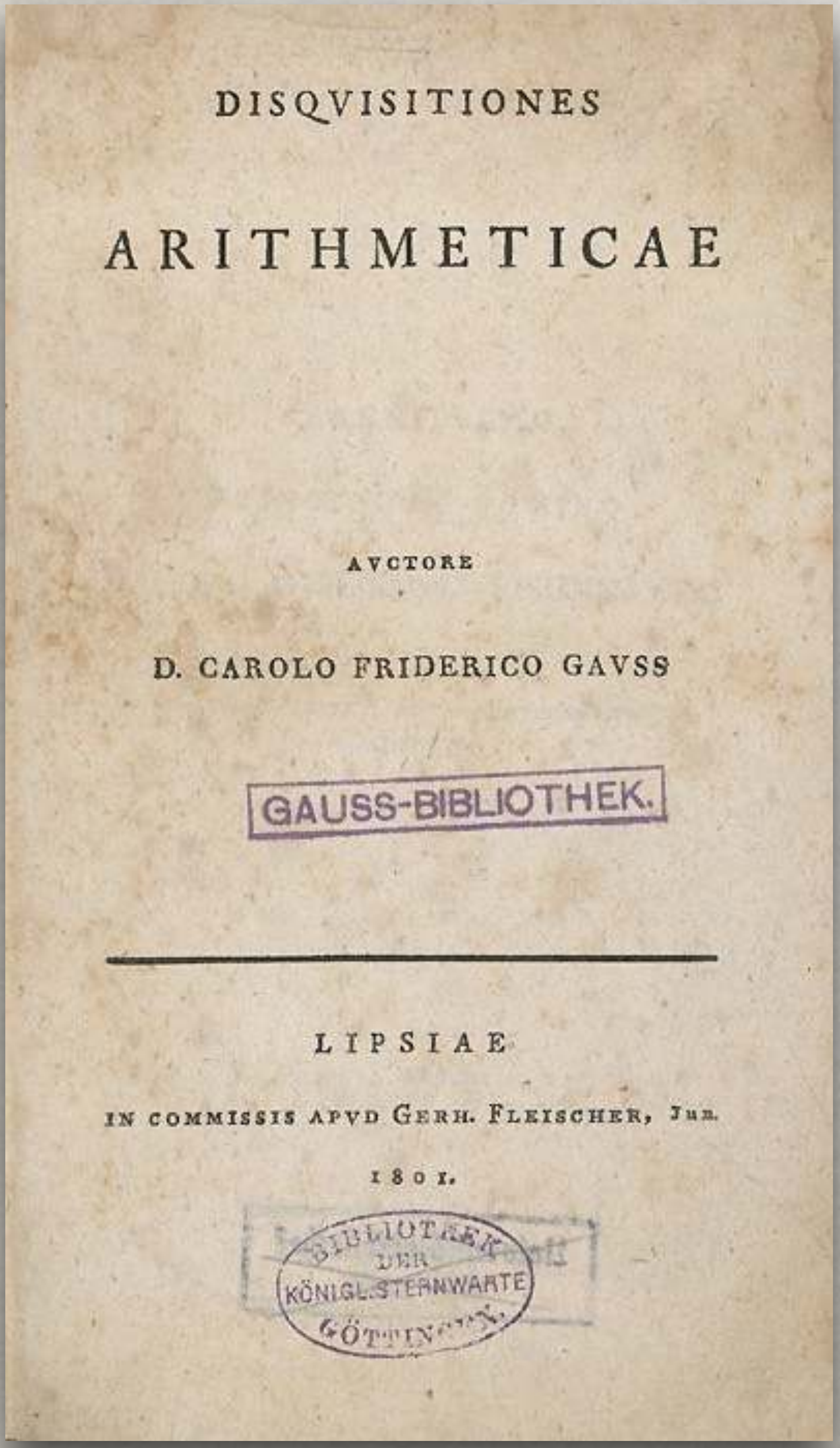
LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, IVN.

1801.

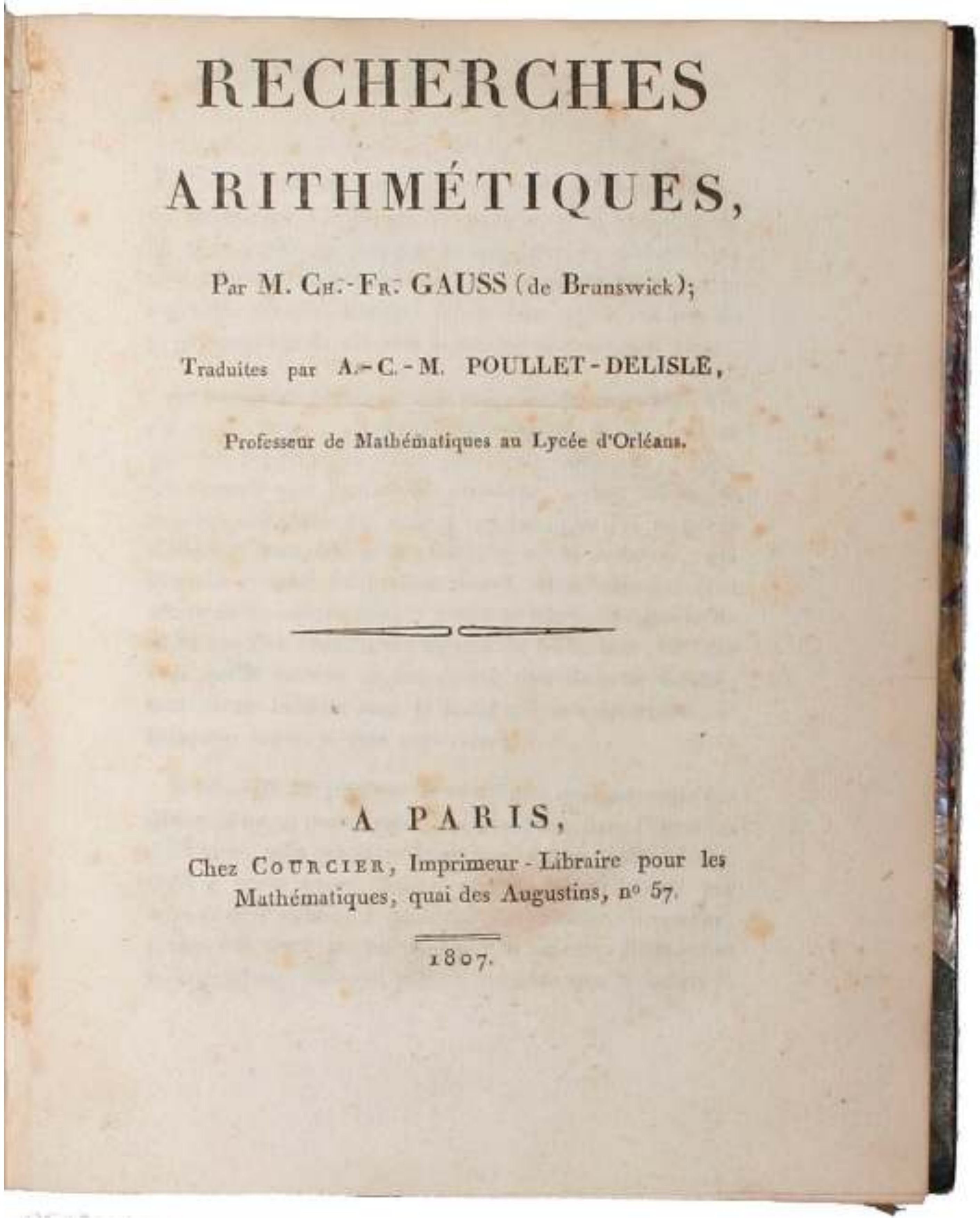
Carl Friedrich Gauss (1777-1855)

portrait par J.C.A. Schwartz, 1803



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.

À PARIS,

Chez COURCIER, Imprimeur-Libraire pour les Mathématiques, quai des Augustins, nº 57.

1807.

Traduction française : 1807

RECHERCHES

Carl Friedrich Gauss'

Untersuchungen über höhere Arithmetik.

(Disquisitiones arithmeticae. Theorematis arithmetici demonstratio nova. Summatio quarundam seriorum 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.

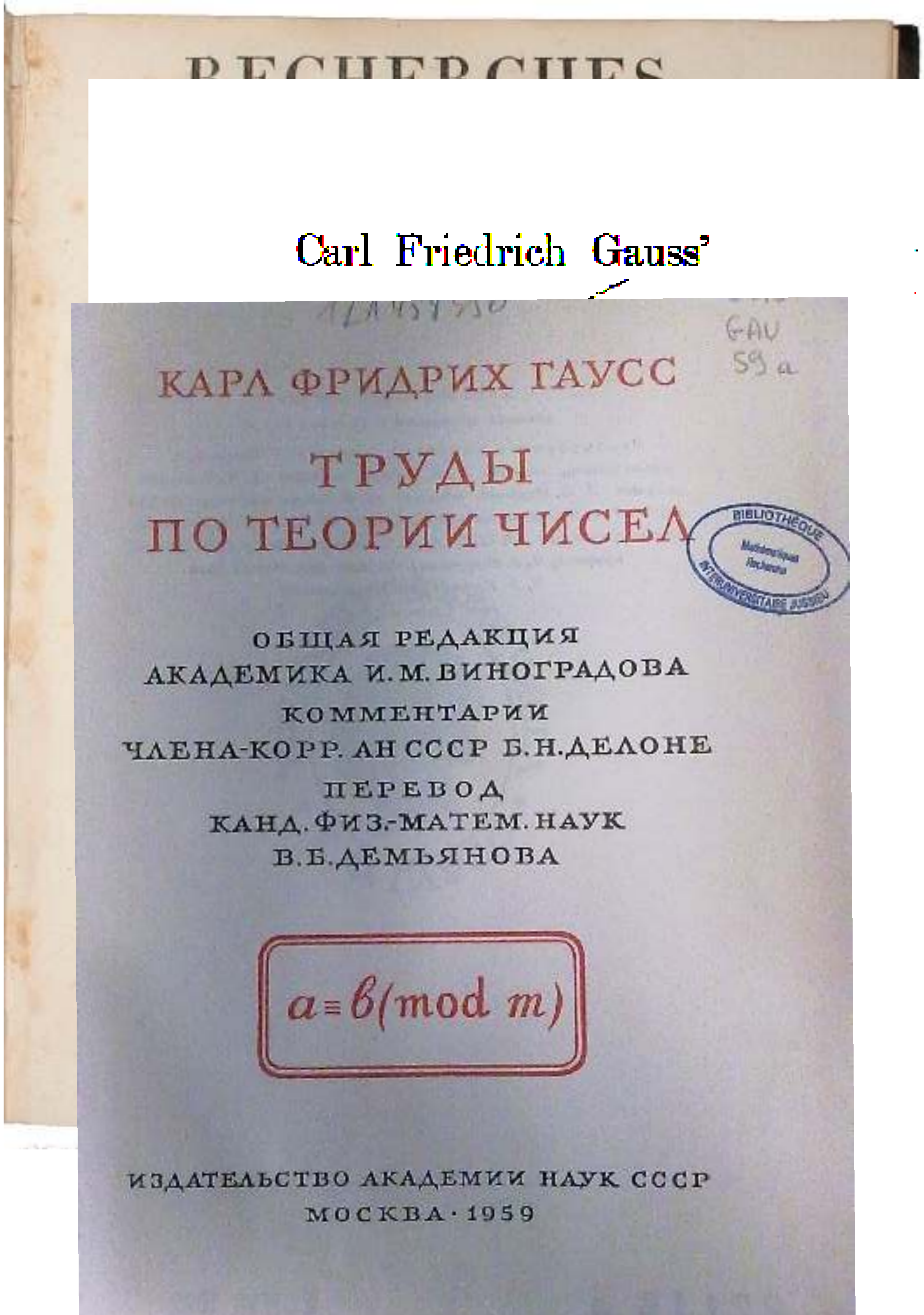
Berlin.

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.

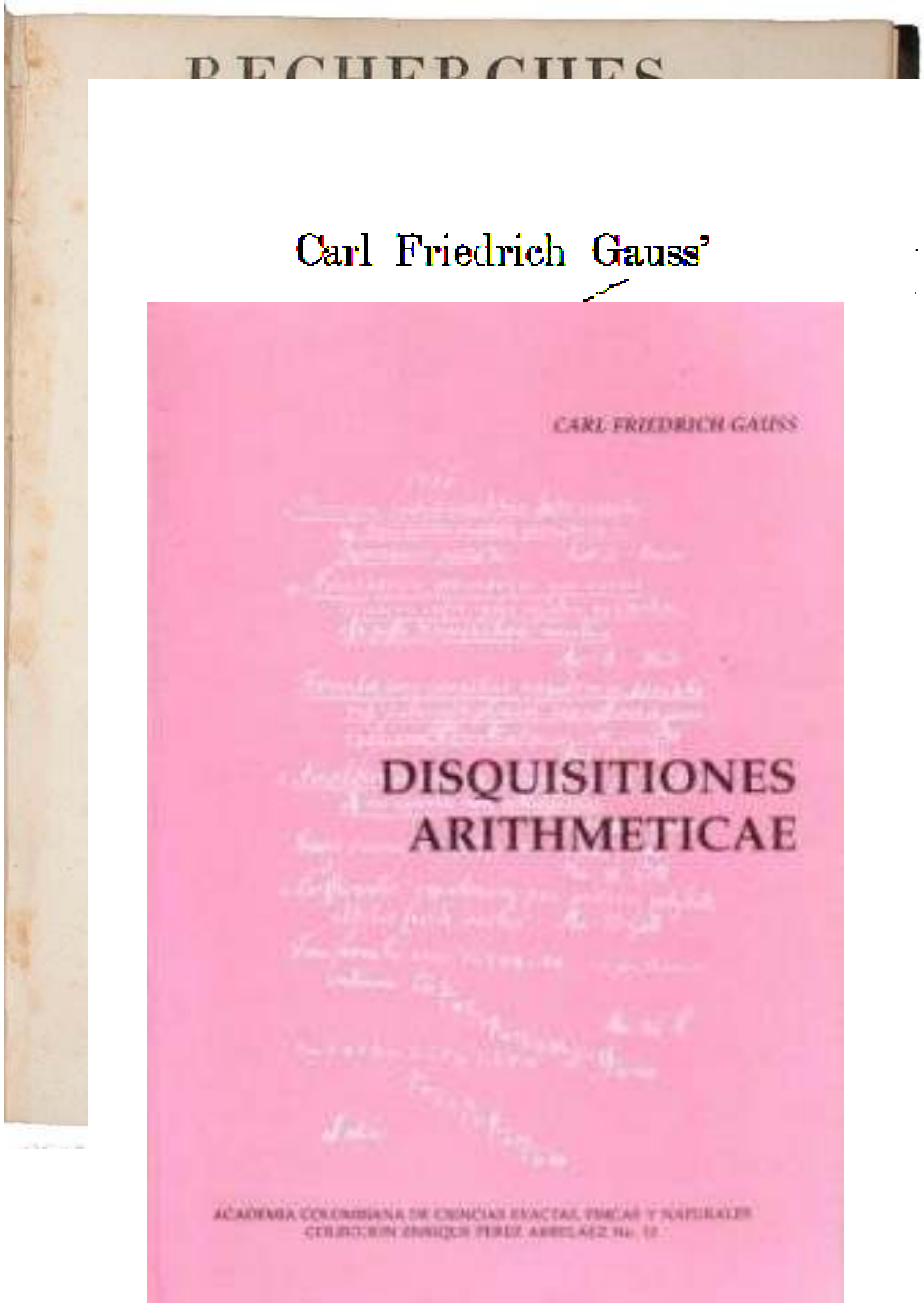
NEW HAVEN AND LONDON, YALE UNIVERSITY PRESS, 1966

Traduction française : 1807

Traduction allemande : 1889

Traduction russe : 1959

Traduction anglaise : 1966



Traduction française : 1807

Traduction allemande : 1889

Traduction russe : 1959

Traduction anglaise : 1966

Traduction castillane : 1995

Traduction française : 1807

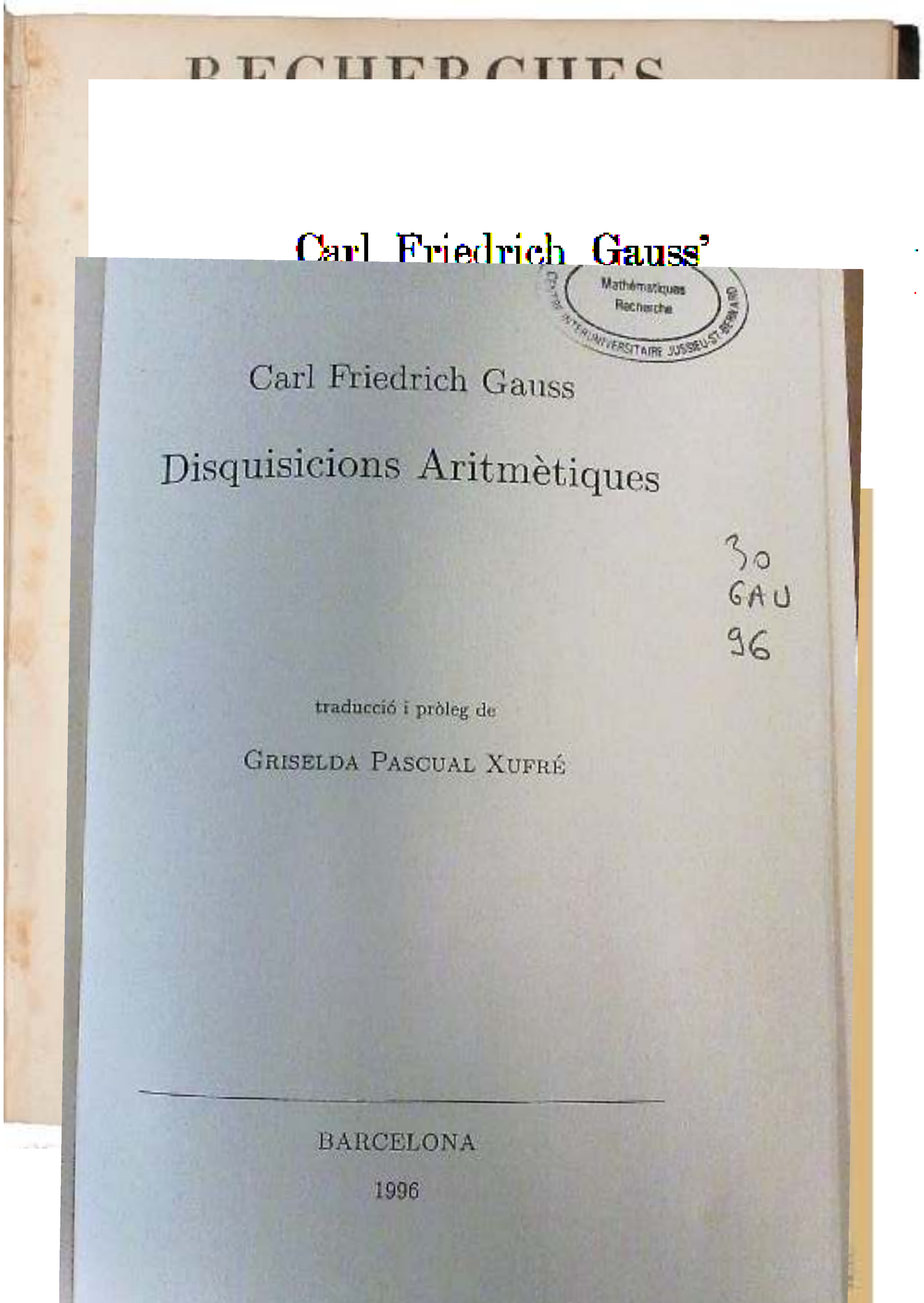
Traduction allemande : 1889

Traduction russe : 1959

Traduction anglaise : 1966

Traduction castillane : 1995

Traduction japonaise : 1995



Traduction française : 1807

Traduction allemande : 1889

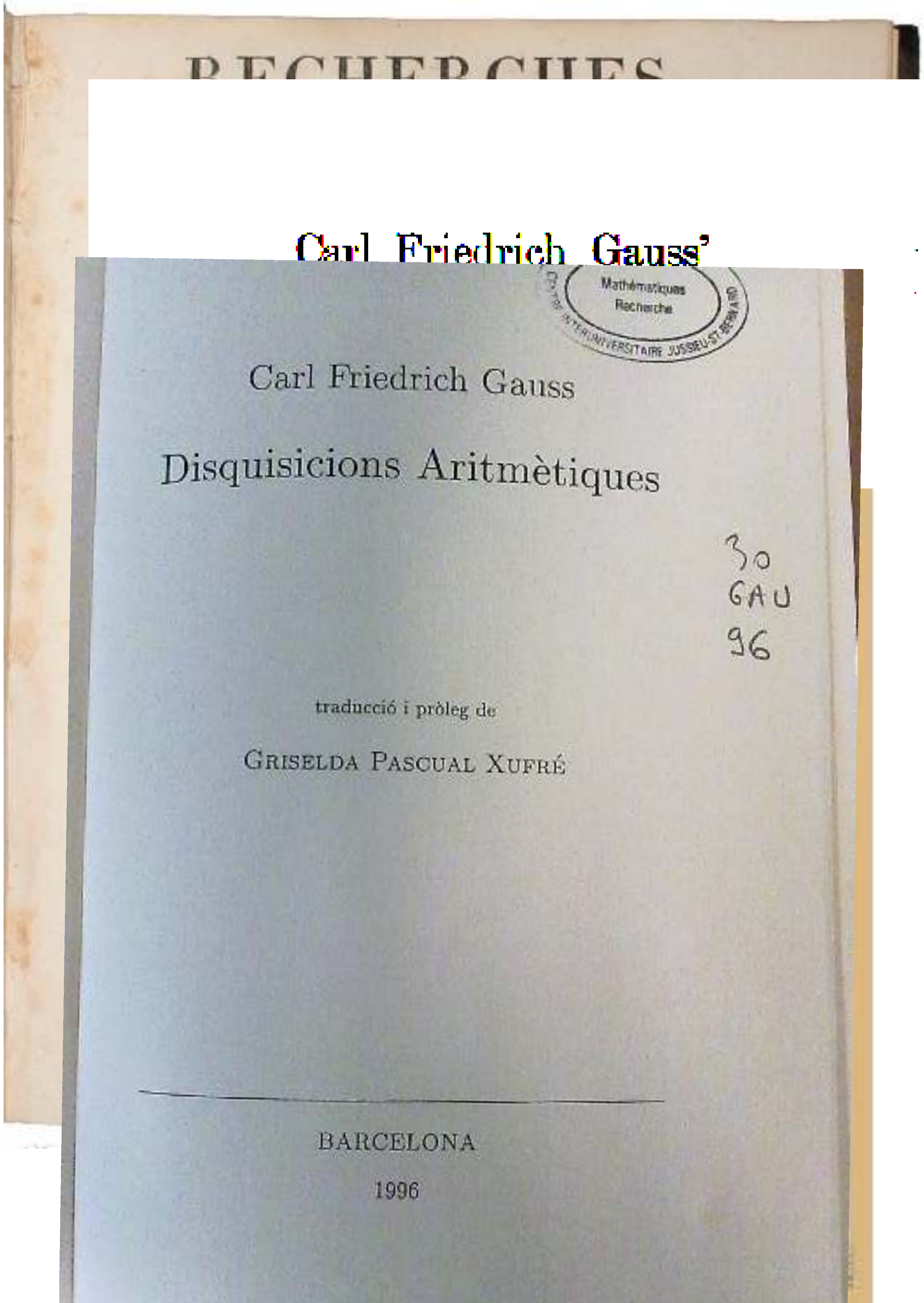
Traduction russe : 1959

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

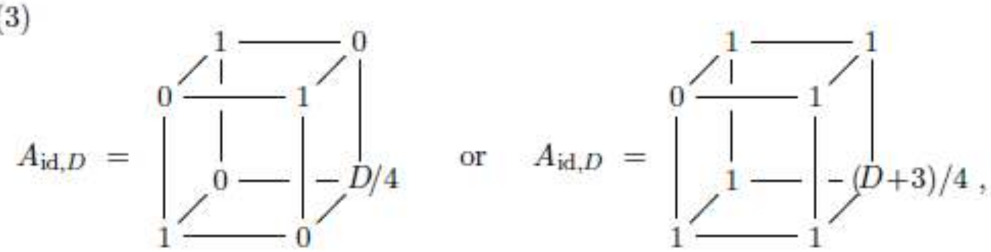
Traduction japonaise : 1995

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

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

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

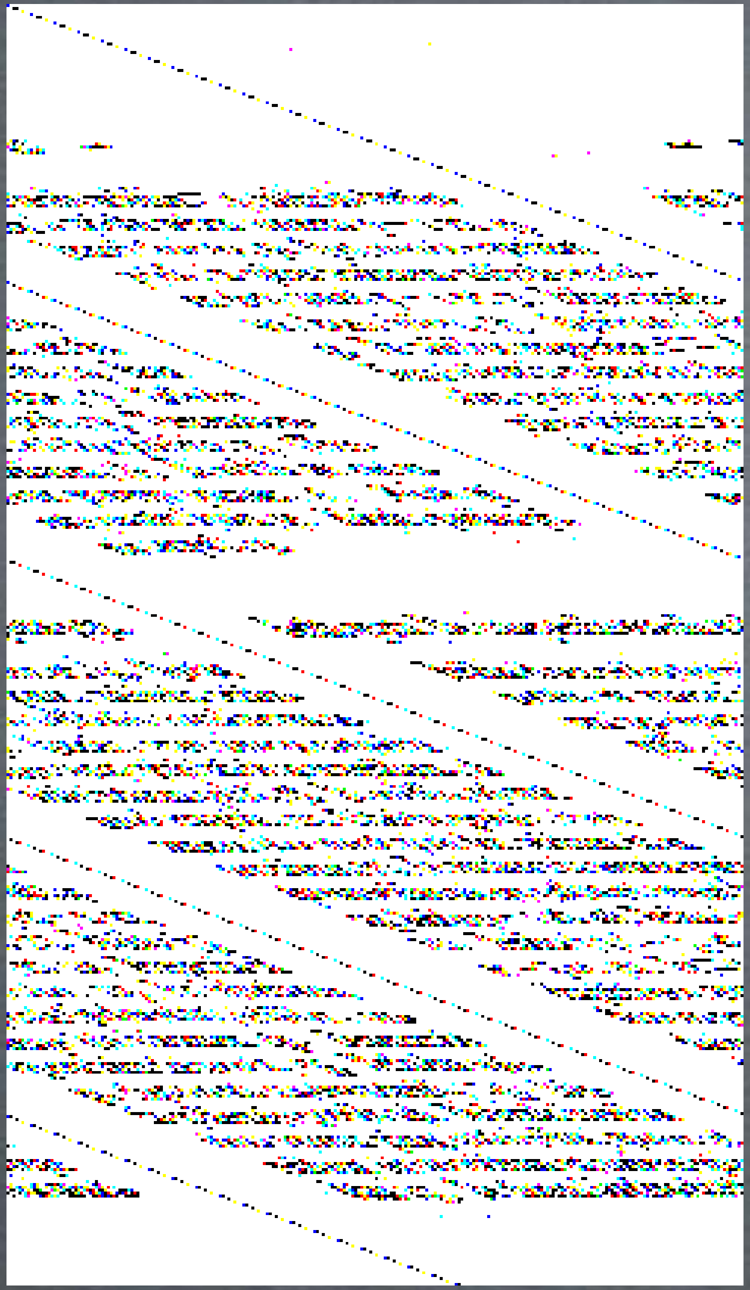
Received by the editors October 2, 1948; published with the invited addresses for reasons of space and editorial convenience.

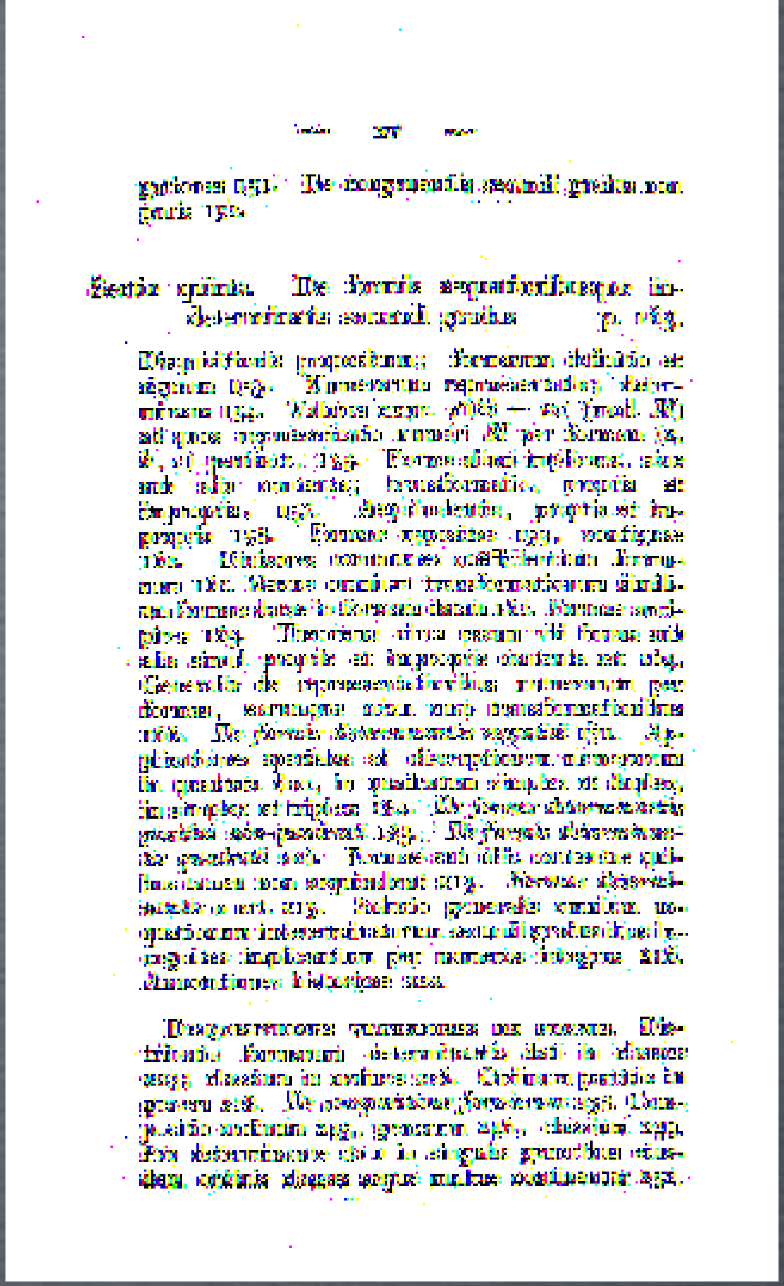
[1] Numbers in brackets refer to the bibliography at the end of the paper.

[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-$by^3 \equiv 1$ (mod p)

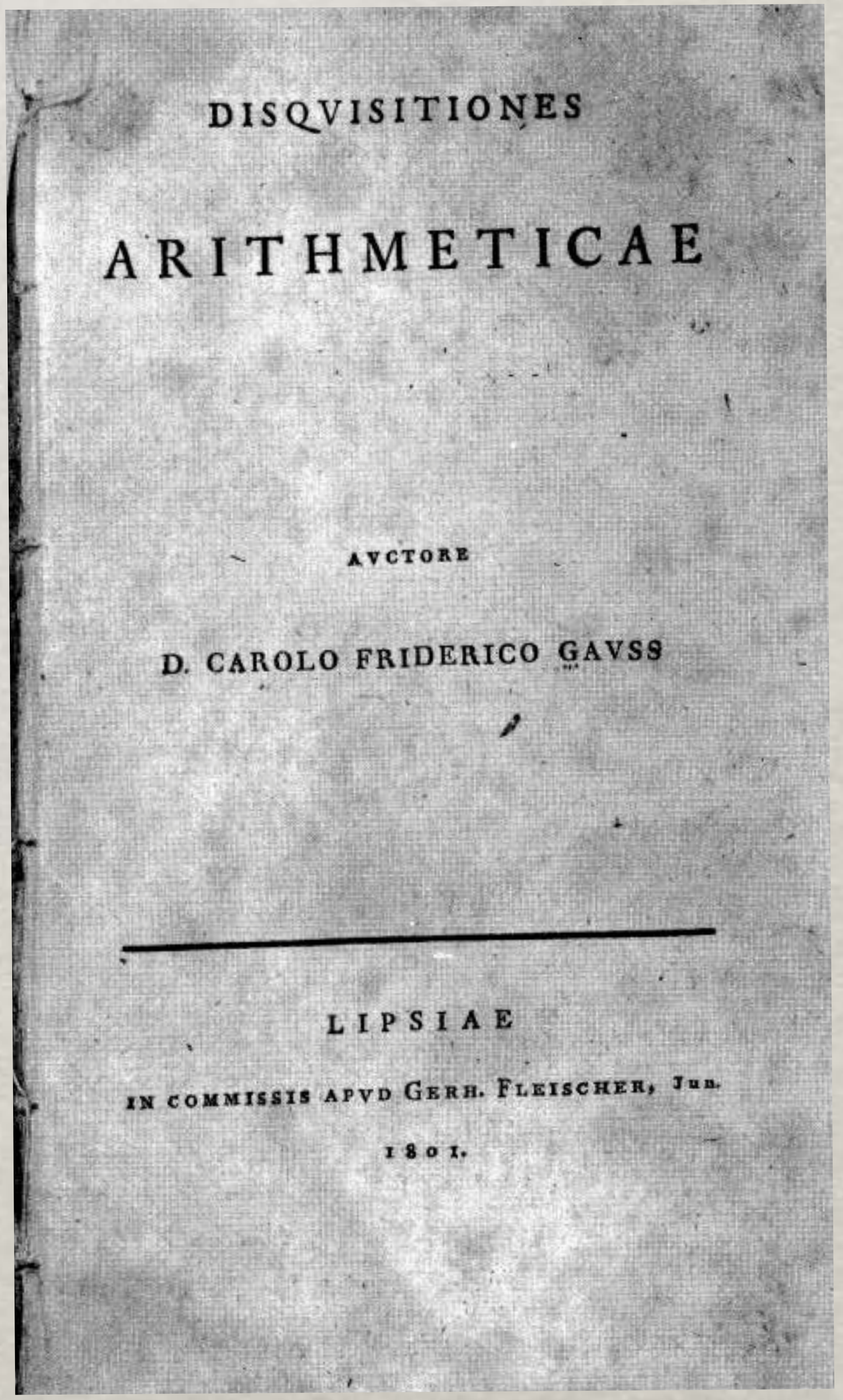




LA STRUCTURE DES DISQUISITIONES ARITHMETICAE

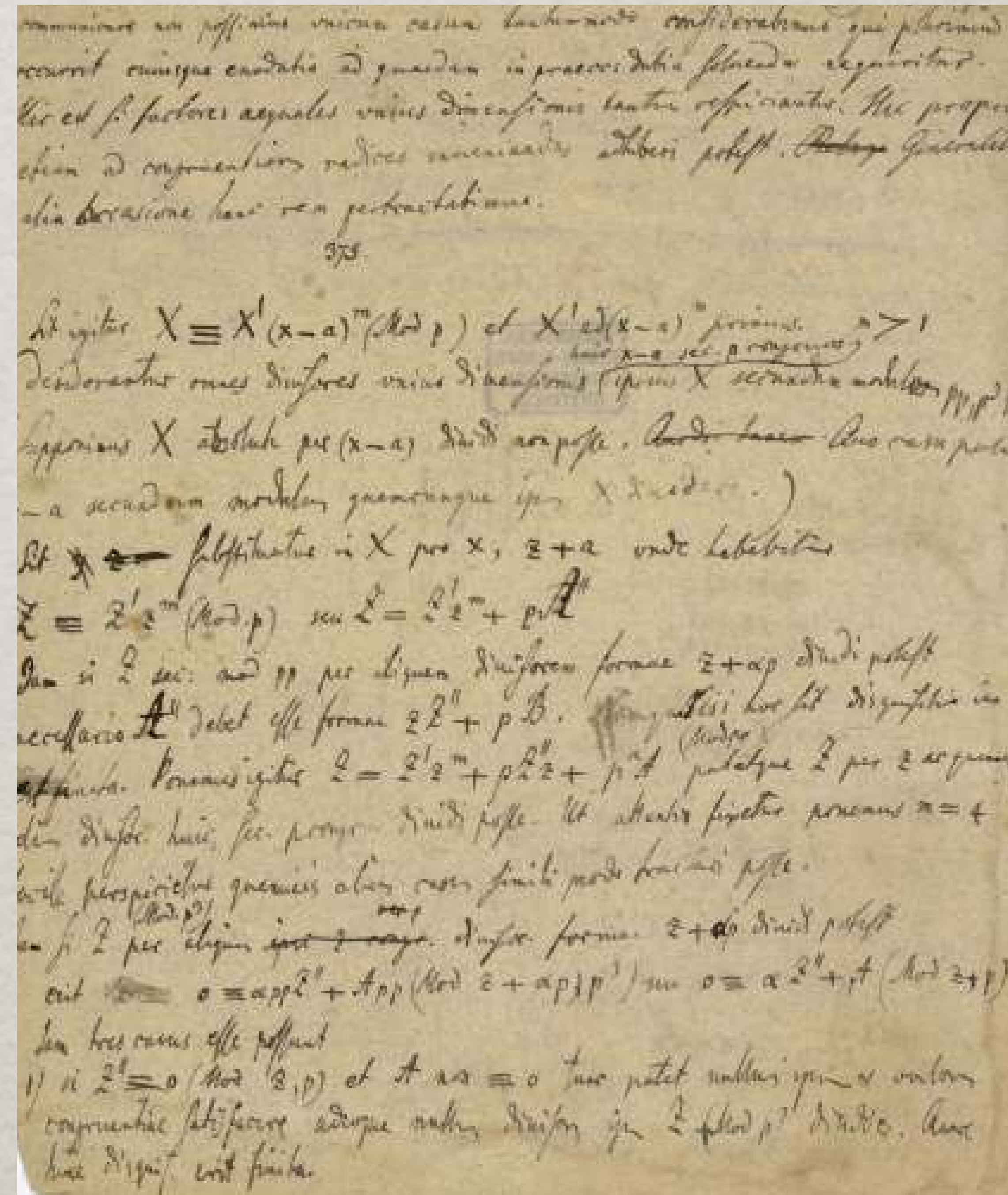
LES D.A. EN 1801

- "Les entiers… constituent l'objet propre de l'arithmétique."
- 665 pages
- 355 articles
- *7* sections ("les sept sceaux")



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

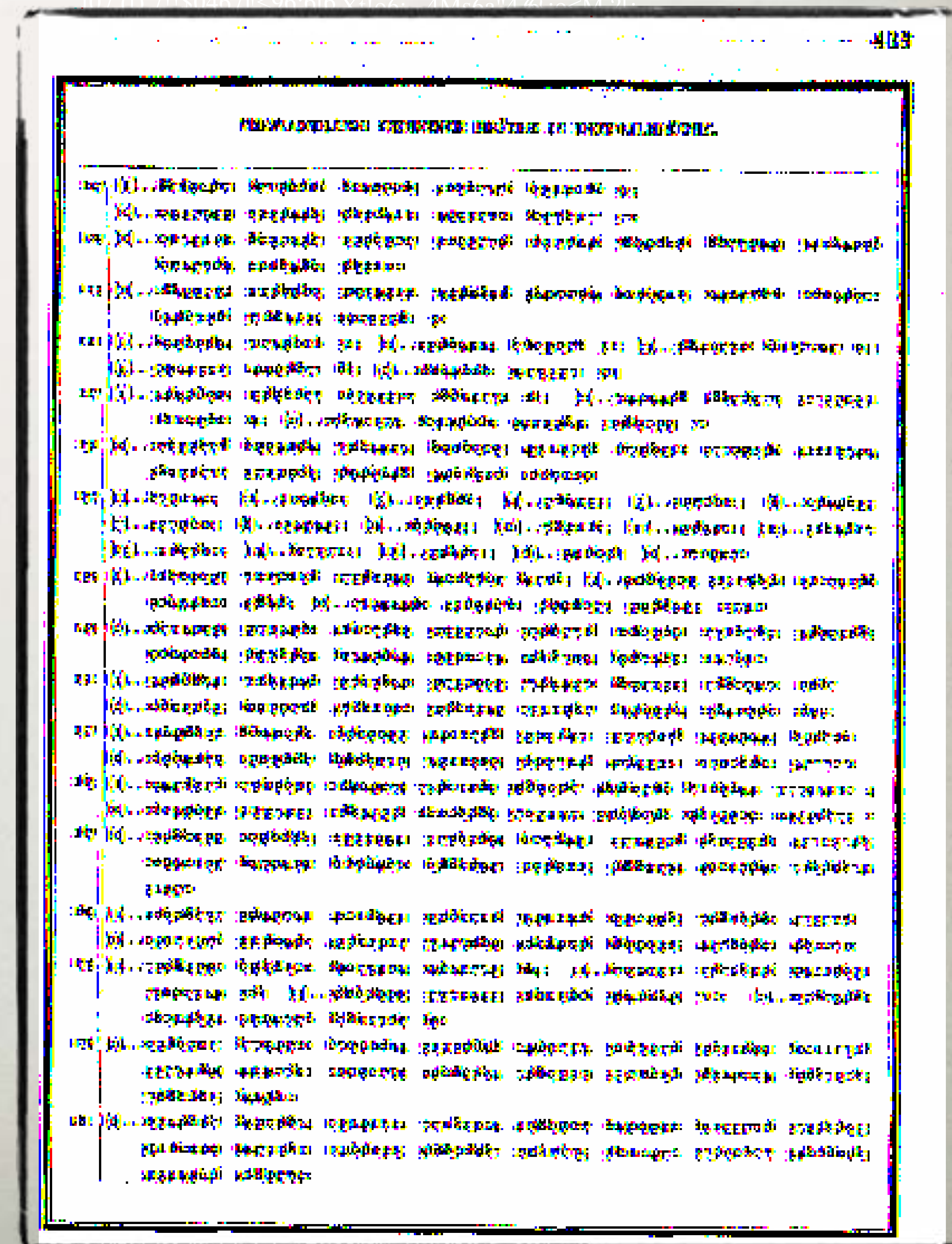
En mécanique, on a depuis longtemps utilisé [ce principe de périodicité] comme source d'invention des machines, parce que chaque retour périodique de transformations peut être engendré par des machines et chaque ordre local dans une série de changements devient périodique.

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

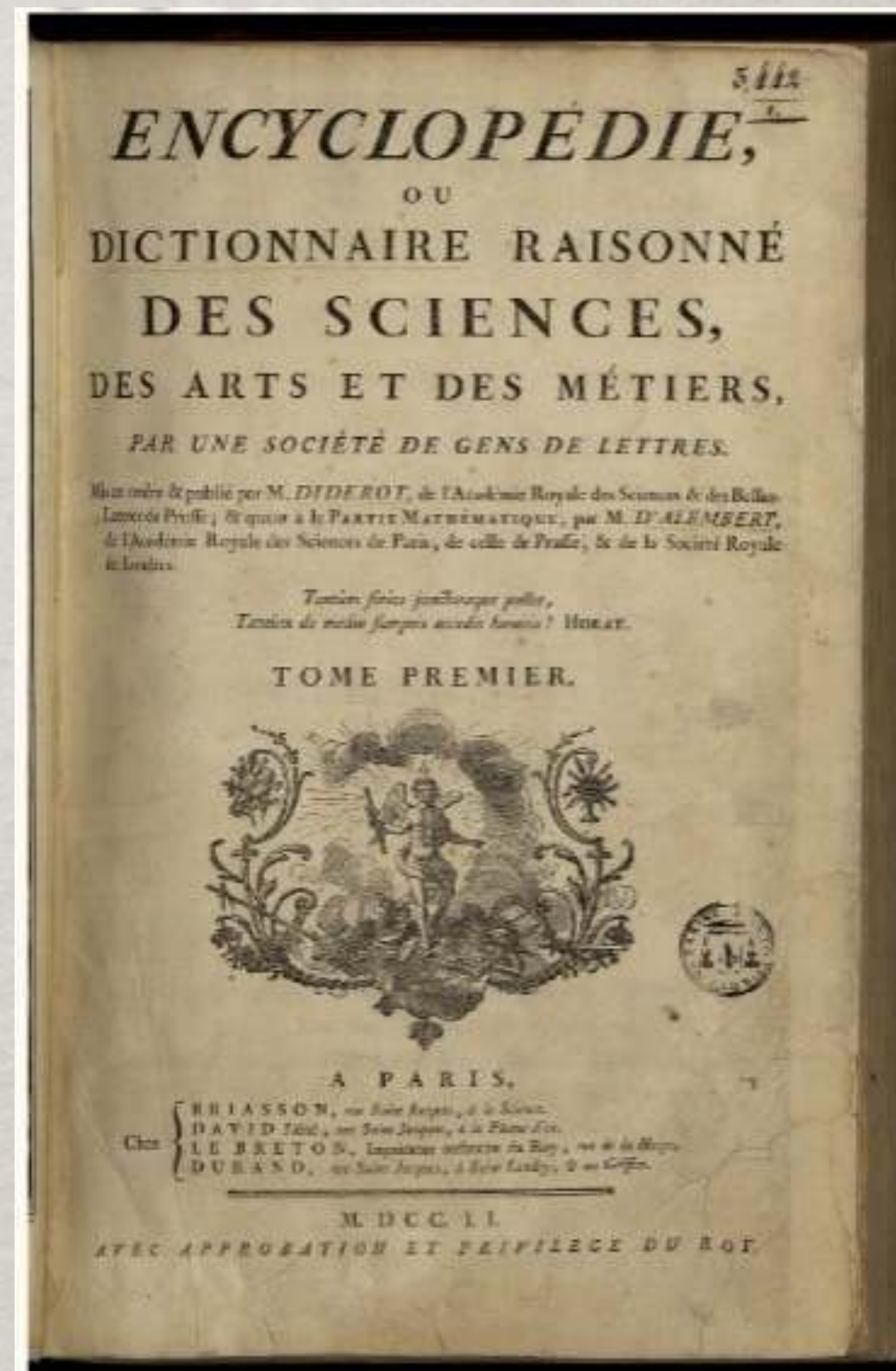
- Nombres congrus
- Congruences du premier degré
- Résidus de puissances
- Congruences du second degré
- Formes et équations indéterminées du second degré
- Applications variées
- Sur les équations déterminant les divisions du cercle

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*]

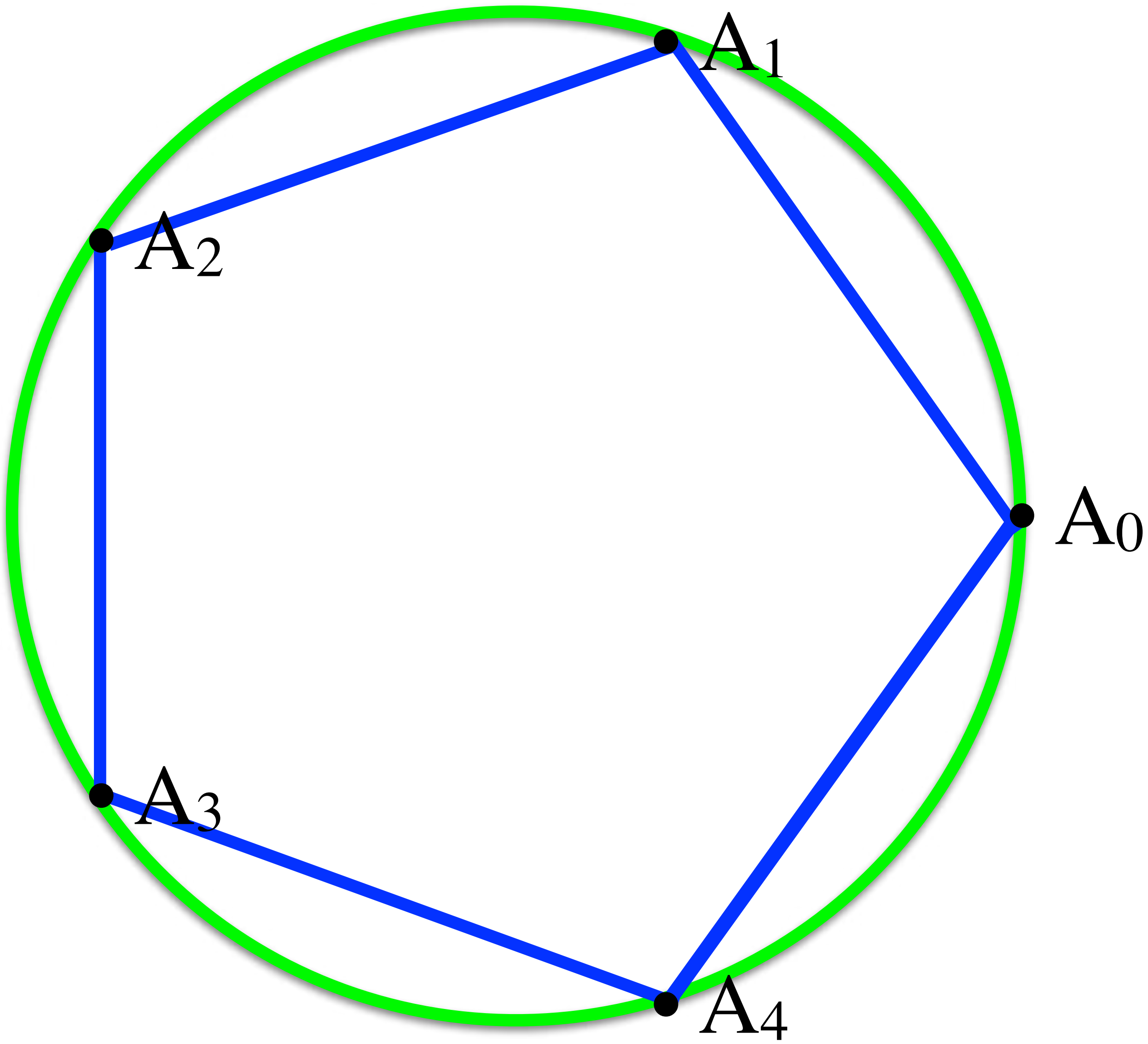
EFFECTIF, adj. qui est réel & positif. Dans le Commerce, un payement effectif est celui qui se fait véritablement & en deniers comptans, ou effets équivalens.

[G : Edme François Mallet, *Encyclopédie*]



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

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



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

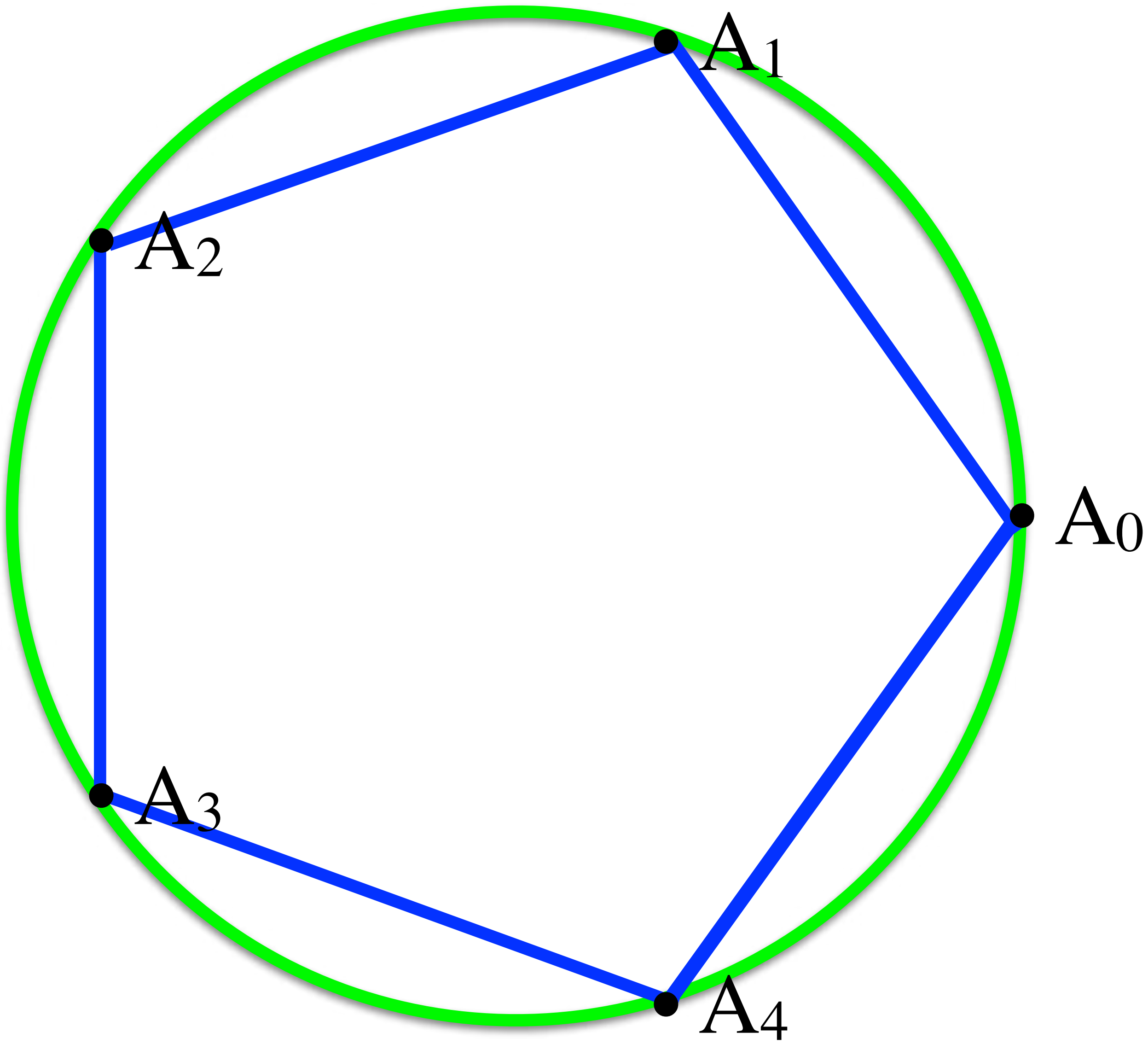
A_1 : $(\cos 2\pi/5, \sin 2\pi/5) = \exp(2\pi i/5)$

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 $x^5-1=0$

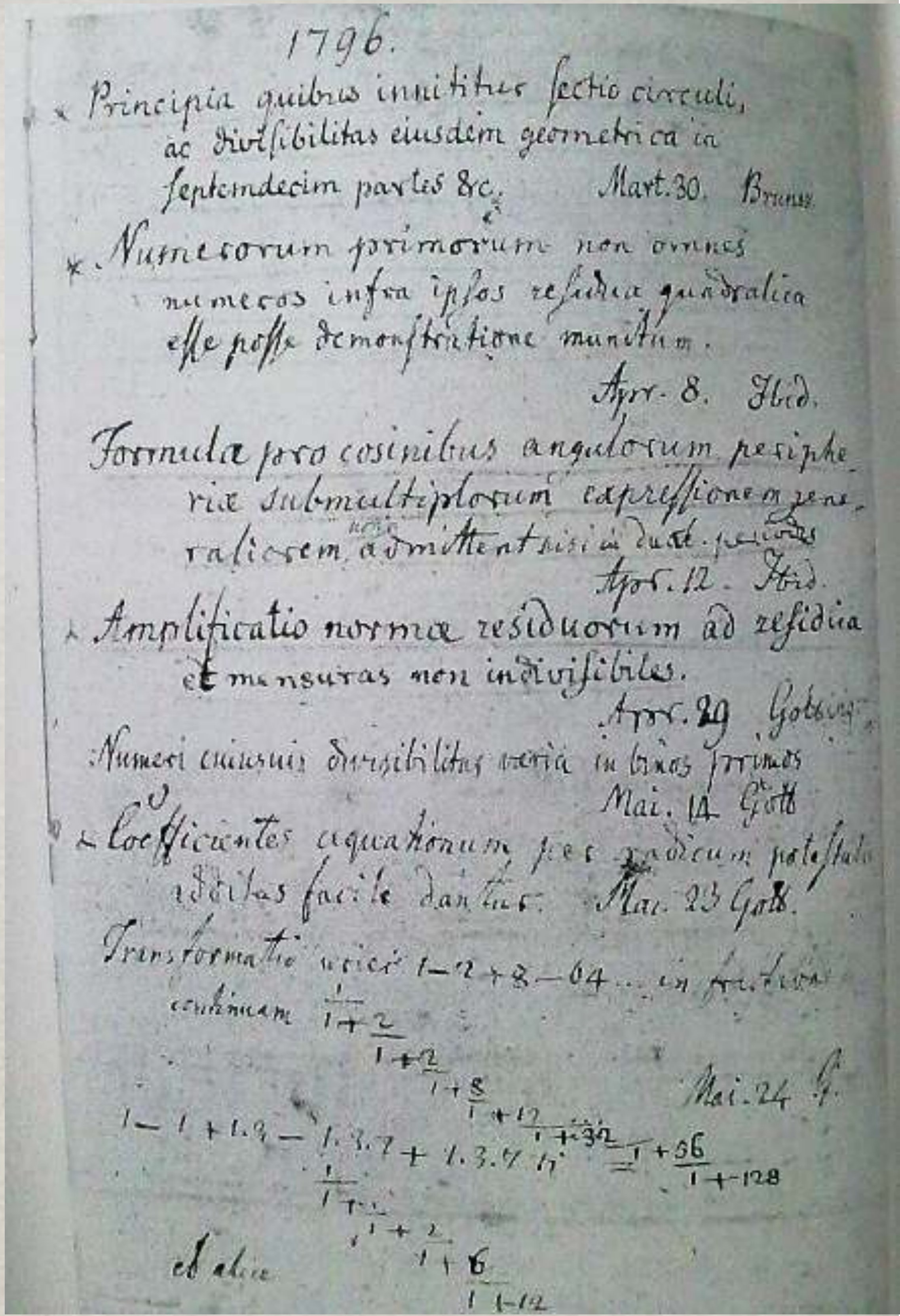
"On trouve donc, en-dessous de 300, les 38 valeurs suivantes pour le nombre N [tel qu'un polygone régulier à N côtés soit inscriptible à la règle et au compas dans un cercle] :
2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170,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


1796.
Principia quibus innititur sectio circuli, ac divisibilitas eiusdem geometrica in septemdecim partes &c. Mart. 30. Brunsv.
Numerorum primorum non omnes numeros infra ipsos residua quadratica esse posse demonstratione munitum. Apr. 8. Ibid.
Formula pro cosinibus angulorum peripheriae submultiplorum expressionem generaliorem non admittentibus ... Apr. 12. Ibid.
Amplificatio normae residuorum ad residua et mensuras non indivisibiles. Apr. 29 Gotting.
Numeri cuiusuis divisibilitas varia in binos primos. Mai. 14 Gott.
Coefficientes aequationum per radicum potestatum ... facile dantur. Mai. 23 Gott.
Transformatio seriei 1−2+8−64... in fractionem continuam ... Mai. 24 G.
Et alia

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 , $j = 1, 2, \ldots 18$, 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]

$$[6,1] = r+r^7+r^8+r^{11}+r^{12}+r^{18}$$
$$= (r+r^{18})+(r^7+r^{12})+(r^8+r^{11})$$
$$= (r^{2^{18}}+r^{2^9})+(r^{2^6}+r^{2^{15}})+(r^{2^3}+r^{2^{12}})$$

- [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...

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

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

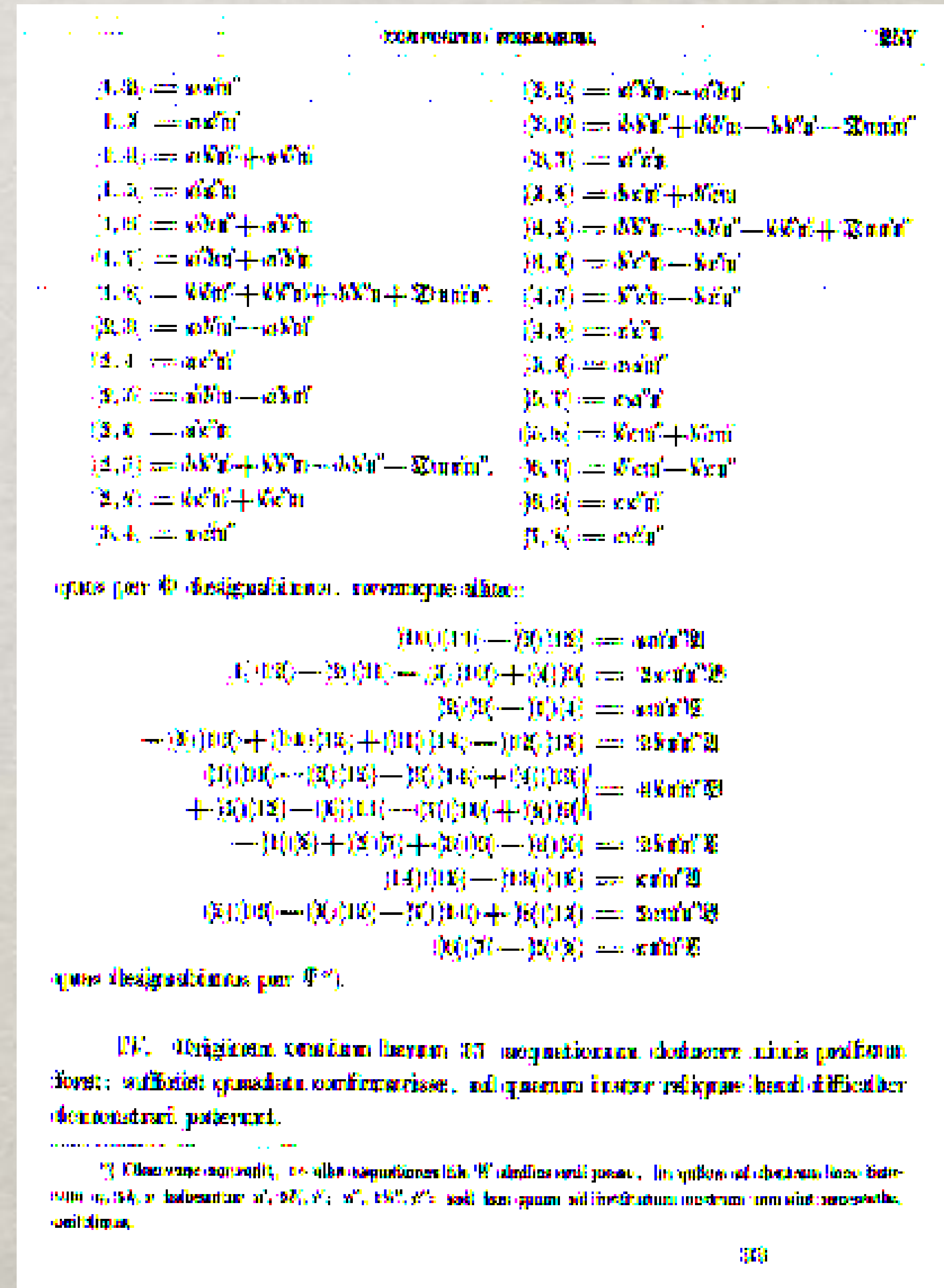
$$\cos\frac{P}{17} = -\tfrac{1}{16} + \tfrac{1}{16}\sqrt{17} + \tfrac{1}{16}\sqrt{(34 - 2\sqrt{17})} - \tfrac{1}{8}\sqrt{\{(17 + 3\sqrt{17}) - \sqrt{(34 - 2\sqrt{17})} - 2\sqrt{(34 + 2\sqrt{17})}\}};$$

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 $\alpha, \beta, \cdots, \lambda$, tels que

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

• 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 :

$| m' - Am |< \frac{2}{\sqrt{3}}\frac{1}{\sqrt[6]{\Delta}}$, $| m'' - Bm |< \frac{2}{\sqrt{3}}\frac{1}{\sqrt[6]{\Delta}}$, $| m |< \frac{2}{\sqrt{3}}\sqrt[3]{\Delta}$.

Ou encore :

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

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

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