

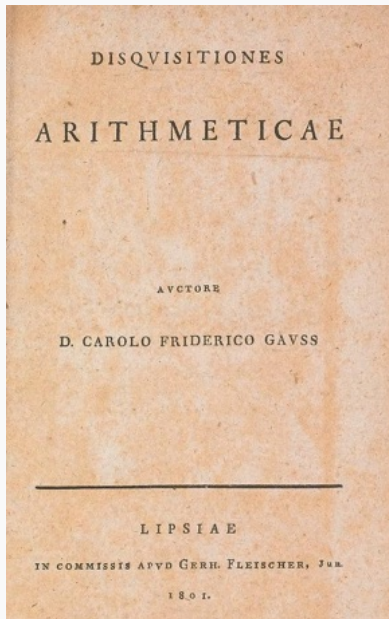
# Des formes et des idéaux : aperçus sur la théorie des nombres au XIX<sup>e</sup> siècle

---

François Lê  
Université Claude Bernard Lyon 1  
Institut Camille Jordan

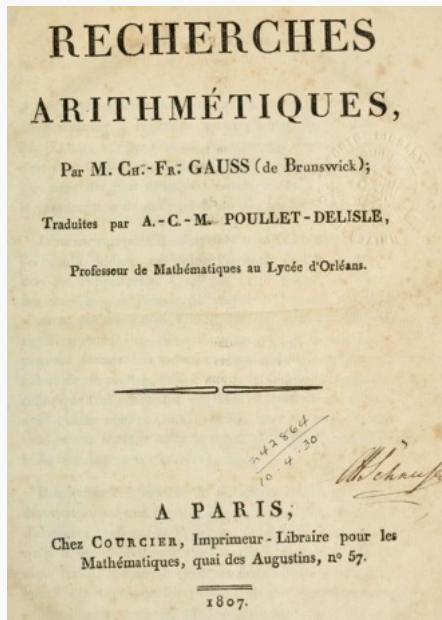
15 novembre 2025

# *Disquisitiones arithmeticae*, 1801



Carl Friedrich Gauss (1777-1855)

# Disquisitiones arithmeticae, 1801



« 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. » (Legendre, 1804)

« Ce livre, monument impérissable, dévoile l'immense étendue, l'étonnante profondeur de la pensée humaine. » (Lucas, 1891)

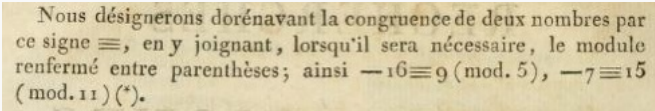
« C'est un ouvrage qui a en mathématiques à peu près la même position que la *Critique de la raison pure* de Kant en philosophie. » (Itzigsohn, 1885)

# Structure du livre

- ▶ 665 pages, 7 sections :
  - I. Des nombres congrus en général
  - II. Des congruences du premier degré
  - III. Des résidus de puissances
  - IV. Des congruences du second degré
  - V. Des formes et des équations du second degré
  - VI. Applications des recherches précédentes
  - VII. Des équations qui déterminent la division du cercle

# Congruences et résidus

- Définition et notation  $\equiv$ , utilisée « à cause de la grande analogie qui existe entre l'égalité et la congruence ».



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  $-16 \equiv 9 \pmod{5}$ ,  $-7 \equiv 15 \pmod{11}$  (\*).

- Progressions géométriques  $1, a, a^2 \dots$  modulo un nombre premier  $p$ .
  - Si  $\text{pgcd}(a, p) = 1$ , on a  $a^{p-1} \equiv 1 \pmod{p}$ .
  - « Il existe des nombres dont aucune puissance plus petite que  $p - 1$  est congruente à 1 modulo  $p$ . »  $\rightsquigarrow (\mathbf{Z}/p\mathbf{Z})^\times$  est cyclique.
- Résidus quadratiques  $a$  modulo  $p$  : il existe  $x$  tel que  $a \equiv x^2 \pmod{p}$ .
  - Loi de réciprocité quadratique : soient  $p$  et  $q$  premiers impairs distincts.
    - Si  $p$  ou  $q \equiv 1 \pmod{4}$ ,  $p$  est résidu mod  $q$  ssi  $q$  est résidu mod  $p$ ;
    - Si  $p$  et  $q \equiv 3 \pmod{4}$ ,  $p$  est résidu mod  $q$  ssi  $q$  n'est pas résidu mod  $p$ .

# Cyclotomie (section VII)

- Équation cyclotomique  $\frac{x^p-1}{x-1} = x^{p-1} + \dots + x + 1 = 0$ , de racines  $\alpha, \alpha^2, \dots, \alpha^{p-1}$  avec  $\alpha = e^{2i\pi/p} = \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p}$ .
- Est-elle résoluble (par radicaux)?
- Clé : les racines sont écrites  $\alpha^{g^1}, \alpha^{g^2}, \dots, \alpha^{g^{p-1}}$ , où  $g$  engendre  $(\mathbf{Z}/p\mathbf{Z})^\times$ .
- Le polygone régulier à 17 côtés est constructible à la règle et au compas.

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

- Le polygone régulier à 19 côtés ne l'est pas.



# Formes quadratiques binaires (section V)

- Étude des expressions  $ax^2 + 2bxy + cy^2$  avec  $a, b, c$  entiers.
- Problème 1 : détermination des entiers représentables par une forme donnée.
  - 29 est de la forme  $x^2 + y^2$  car  $29 = 2^2 + 5^2$ .
  - 29 est aussi de la forme  $5x^2 + 26xy + 34y^2$  :
    - On a  $5x^2 + 26xy + 34y^2 = (2x + 5y)^2 + (x + 3y)^2$ ;
    - Il existe  $x, y$  tels que

$$\begin{cases} 2 = 2x + 5y \\ 5 = x + 3y \end{cases}$$

$$\text{car } \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \in \text{GL}_n(\mathbf{Z}), \text{ puisque } 2 \cdot 3 - 5 \cdot 1 = \pm 1.$$

# Classifier les formes quadratiques

- Problème 2 : classification des formes à changement de variable près.
  - $f = ax^2 + 2bxy + cy^2$  et  $f' = a'x^2 + 2b'xy + c'y^2$  sont équivalentes s'il existe  $\alpha, \beta, \gamma, \delta$  entiers tels que

$$f(\alpha x + \beta y, \gamma x + \delta y) = f'(x, y).$$

et  $\alpha\delta - \beta\gamma = \pm 1$ .

- Permet de regrouper les formes en classes.
  - Représentants privilégiés des classes, nombre de classes, loi de composition entre classes...
- Extension aux formes ternaires.
  - Applications : loi de réciprocité quadratique, tout nombre  $8n + 3$  est de la forme  $x^2 + y^2 + z^2 \dots$

# Les *Disquisitiones* et la théorie des nombres au XIX<sup>e</sup> siècle

- ▶ Années 1800-1820 : réception des *Disquisitiones* surtout en lien avec la section VII (cyclotomie).
- ▶ Années 1830-1860 : champ de recherches qui mêle :
  - Arithmétique (congruences, lois de réciprocité, formes...);
  - Algèbre (équations, utilisation des nombres complexes...);
  - Analyse (séries, séries de Fourier, fonctions elliptiques...),avec Jacobi, Dirichlet, Kummer, Eisenstein, Hermite, Kronecker...
- ▶ Années 1870-1910 : trois principales lignes de recherche :
  - Questions de congruences, nombres premiers, loi de réciprocité quadratique.
  - Utilisations de fonctions complexes, dans la lignée de Dirichlet.
  - Théorie arithmétique des formes, équations modulaires, dans la lignée de Hermite et Kronecker.
- ▶ Années 1850-1910 : petit nombre de recherches sur les idéaux, corps de nombres, etc. (Dedekind, Kronecker, Hurwitz, Hilbert...).

# Formes arithmétiques

---

# Des formes arithmétiques après Gauss

- ▶ Formes quadratiques avec  $n$  variables (à coefficients dans  $\mathbf{Z}$ ).
- ▶ Formes binaires de degré  $m$  (à coefficients dans  $\mathbf{Z}$ ).
- ▶ Formes à  $n$  variables et de degré  $m$  (à coefficients dans  $\mathbf{Z}$ ).
- ▶ Formes avec d'autres types de coefficients : réels, complexes en lien avec questions arithmétiques (entiers de Gauss  $a + ib \in \mathbf{Z}[i]$ ).
- ▶ Questions de classification, détermination des nombres de classes, de représentations de nombres.

# Le théorème des minima d'Hermite

- 1850, Hermite considère une forme quadratique réelle définie

$$f = a_{11}x_1^2 + 2a_{12}x_1x_2^2 + \cdots + a_{nn}x_n^2.$$

- Si  $D$  est le déterminant de  $f$ , il existe  $x_1, \dots, x_n$  entiers non tous nuls tels que

$$|f(x_1, \dots, x_n)| \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} \sqrt[n]{|D|}.$$

- Nombreuses applications :

- Approximation simultanée de réels par des rationnels.
- Une fonction entière de  $n$  variables ne peut pas avoir plus de  $2n$  périodes.
- Décomposition d'un nombre premier comme produit d'entiers cyclotomiques.
- Théorème des quatre carrés.



Charles Hermite (1822-1901)

# Le théorème des quatre carrés

- Théorème : tout entier positif  $A$  est somme de quatre carrés :

$$A = a^2 + b^2 + c^2 + d^2.$$

- Soit  $A$  non divisible par 4.
- Lemme : il existe  $\alpha, \beta$  entiers tels que  $\alpha^2 + \beta^2 \equiv -1 \pmod{A}$ .
- Soit  $f(x, y, z, u) = (Ax + \alpha z + \beta u)^2 + (Ay - \beta z + \alpha u)^2 + z^2 + u^2$ .

- Les valeurs de  $f$  aux entiers sont multiples de  $A$ .
- $f$  est de déterminant  $A^4$ .
- Par le théorème des minima, il existe  $x, y, z, u$  non tous nuls tels que

$$|f(x, y, z, u)| \leq \left(\frac{4}{3}\right)^{3/2} \sqrt[4]{A^4} \simeq 1,54 A.$$

- Donc  $A = f(x, y, z, u)$  : c'est une somme de quatre carrés.
- Rq : c'est par là qu'arrivent les formes hermitiennes...

# Nombres algébriques

---

# L'équation de Fermat $x^n + y^n = z^n$

- ▶ 1753/1770, Euler « démontre » le théorème de Fermat pour  $n = 3$ .
  - Si  $x^3 + y^3 = z^3$  avec  $x$  et  $y$  impairs, il existe  $a, b$  tq  $x + y = 2a$  et  $x - y = 2b$ .
  - Alors  $2a(a^2 + 3b^2) = z^3$ , et donc

$$2a(a + ib\sqrt{3})(a - ib\sqrt{3}) = z^3.$$

- Or  $a + ib\sqrt{3}$ ,  $a - ib\sqrt{3}$  et  $2a$  sont deux à deux premiers entre eux, donc chacun est un cube...
  - Problème :  $\mathbf{Z}[i\sqrt{3}]$  n'est pas factoriel!
- ▶ Dans la première moitié du XIX<sup>e</sup>, preuves correctes du théorème par Germain ( $n = 2(8m \pm 3)$ ), Legendre et Dirichlet ( $n = 5$ ), Lamé ( $n = 7$ ).



# Cyclotomie et facteurs idéaux

- ▶ 1847, Lamé pense réussir le cas général en partant de la factorisation

$$x^p + y^p = (x + y)(x + \alpha y)(x + \alpha^2 y) \cdots (x + \alpha^{p-1} y),$$

avec  $\alpha = e^{2i\pi/p}$ .

- ▶ Entiers cyclotomiques  $\omega = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{p-1}\alpha^{p-1} \in \mathbf{Z}[\alpha]$ .
- ▶ 1847, Kummer s'intéresse aussi à ces entiers pour trouver des lois de réciprocité supérieures.
- ▶ Définit des entiers cyclotomiques premiers.
- ▶ Un produit de nombres premiers de  $\mathbf{Z}[\alpha]$  peut être divisible par un autre nombre premier.
- ▶ Définit les facteurs complexes idéaux :
  - Pas d'écriture explicite, mais définition par propriétés de divisibilité d'un nombre donné.
  - Permet d'avoir les bonnes propriétés de factorisations.
- ▶ Application au théorème de Fermat pour certains exposants.



Ernst Eduard Kummer  
(1810-1893)

# Corps et idéaux

- ▶ 1871, Dedekind revisite les travaux de Kummer par les notions de corps et d'idéal.
- ▶ « Corps »  $K$ , par ex.  $\mathbf{Q}(i)$ ,  $\mathbf{Q}(\alpha)$ ,  $\mathbf{Q}(\sqrt{5})$ .
- ▶ « Ordre »  $\mathfrak{o}$  des entiers de  $K$ , par ex.  $\mathbf{Z}[i]$ ,  $\mathbf{Z}[\alpha]$ ,  $\mathbf{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ .
- ▶ « Idéal » : « un système  $\mathfrak{a}$  d'éléments de  $\mathfrak{o}$  tel que la somme et la différence de deux nombres de  $\mathfrak{a}$  est encore un nombre de  $\mathfrak{a}$ ; et le produit d'un nombre dans  $\mathfrak{a}$  et d'un nombre dans  $\mathfrak{o}$  est un nombre dans  $\mathfrak{a}$ . »
- ▶ Divisibilité des idéaux, idéaux premiers, etc.



Richard Dedekind  
(1831-1916)

# Vers la théorie algébrique des nombres

- ▶ 1897, Hilbert, *Bericht über die Theorie der algebraischen Zahlkörper*.
- ▶ Grande synthèse sur l'arithmétique des corps de nombres.
- ▶ Reprise des points de vue de Dedekind et de Kronecker.
- ▶ Très grande influence au  $xx^e$  siècle, surtout dans la constitution de la « théorie algébrique des nombres ».



David Hilbert (1862-1943)

# Et la géométrie ?

- ▶ Liens entre théorie des nombres et géométrie relativement rares au XIX<sup>e</sup> siècle.
- ▶ En particulier, mise en place de la géométrie diophantienne à la fin du siècle :
  - Idée : la recherche des solutions entières de  $x^2 + y^2 = 1$  correspond à celle des points à coordonnées entières du cercle unité.
  - ...
  - 1901 : Poincaré, « Sur les propriétés arithmétiques des courbes algébriques ».
  - ...
  - 1928 : Weil, « L'arithmétique sur les courbes algébriques ».



Henri Poincaré (1854-1912)



André Weil (1906-1998)

Merci pour votre attention !

# The Shaping of Arithmetic

**after** C.F. Gauss's  
**Disquisitiones Arithmeticae**

Catherine Goldstein  
Norbert Schappacher  
Joachim Schwermer

---

Editors

 Springer