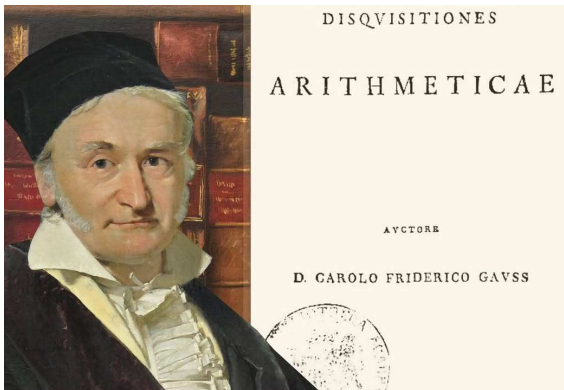


Jean-Christophe San Saturnino



DISQUISITIONES ARITHMETICÆ

mardi 3 février 2026



Le contexte des Disquisitiones

L'enfance de Gauss

- 1777 : Naissance le 30 avril à Brunswick

Le contexte des Disquisitiones

L'enfance de Gauss

- 1777 : Naissance le 30 avril à Brunswick
- 1784 : Entrée à la Katharinen-Volksschule
Enseignants : Büttner et Bartels

Le contexte des Disquisitiones

L'enfance de Gauss

- 1777 : Naissance le 30 avril à Brunswick
- 1784 : Entrée à la Katharinen-Volksschule
Enseignants : Büttner et Bartels
- 1788 : Entrée au Gymnasium Katharineum

Le contexte des Disquisitiones

L'enfance de Gauss

- 1777 : Naissance le 30 avril à Brunswick
- 1784 : Entrée à la Katharinen-Volksschule
Enseignants : Büttner et Bartels
- 1788 : Entrée au Gymnasium Katharineum
- 1791 : Présentation au Duc de Brunswick (bienfaiteur)

Le contexte des Disquisitiones

L'enfance de Gauss

- 1777 : Naissance le 30 avril à Brunswick
- 1784 : Entrée à la Katharinen-Volksschule
Enseignants : Büttner et Bartels
- 1788 : Entrée au Gymnasium Katharineum
- 1791 : Présentation au Duc de Brunswick (bienfaiteur)
- 1792 : Entrée au Collegium Carolinum

Le contexte des Disquisitiones

L'enfance de Gauss

- 1777 : Naissance le 30 avril à Brunswick
- 1784 : Entrée à la Katharinen-Volksschule
Enseignants : Büttner et Bartels
- 1788 : Entrée au Gymnasium Katharineum
- 1791 : Présentation au Duc de Brunswick (bienfaiteur)
- 1792 : Entrée au Collegium Carolinum
- 1795 : Entrée à l'université de Göttingen

Le contexte des Disquisitiones

L'enfance de Gauss

- 1777 : Naissance le 30 avril à Brunswick
- 1784 : Entrée à la Katharinen-Volksschule
Enseignants : Büttner et Bartels
- 1788 : Entrée au Gymnasium Katharineum
- 1791 : Présentation au Duc de Brunswick (bienfaiteur)
- 1792 : Entrée au Collegium Carolinum
- 1795 : Entrée à l'université de Göttingen
- 1796 : Construction de l'heptadécagone

Le contexte des Disquisitiones

L'enfance de Gauss

- 1777 : Naissance le 30 avril à Brunswick
- 1784 : Entrée à la Katharinen-Volksschule
Enseignants : Büttner et Bartels
- 1788 : Entrée au Gymnasium Katharineum
- 1791 : Présentation au Duc de Brunswick (bienfaiteur)
- 1792 : Entrée au Collegium Carolinum
- 1795 : Entrée à l'université de Göttingen
- 1796 : Construction de l'heptadécagone
- 1798 : Doctorat sous la direction de Pfaff à Helmstedt

Le contexte des Disquisitiones

L'enfance de Gauss



Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones

- Vers 300 avant JC : Livres VII à IX des Éléments d'Euclide
divisibilité, nombres premiers, PGCD

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones

- Vers 300 avant JC : Livres VII à IX des Éléments d'Euclide
divisibilité, nombres premiers, PGCD
- IIIe siècle après JC : Les Arithmétiques de Diophante
Résolution d'équations à coefficients dans $\mathbb{Z}$

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones

- Vers 300 avant JC : Livres VII à IX des Éléments d'Euclide
divisibilité, nombres premiers, PGCD
- IIIe siècle après JC : Les Arithmétiques de Diophante
Résolution d'équations à coefficients dans $\mathbb{Z}$
- XVIIe siècle : Fermat

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones

- Vers 300 avant JC : Livres VII à IX des Éléments d'Euclide
divisibilité, nombres premiers, PGCD
- IIIe siècle après JC : Les Arithmétiques de Diophante
Résolution d'équations à coefficients dans $\mathbb{Z}$
- XVIIe siècle : Fermat
 - Petit théorème de Fermat : $a^p \equiv a \pmod{p}$

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones

- Vers 300 avant JC : Livres VII à IX des Éléments d'Euclide
divisibilité, nombres premiers, PGCD
- IIIe siècle après JC : Les Arithmétiques de Diophante
Résolution d'équations à coefficients dans $\mathbb{Z}$
- XVIIe siècle : Fermat
 - Petit théorème de Fermat : $a^p \equiv a \pmod{p}$
 - Grand théorème de Fermat : $x^n + y^n = z^n$

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones

- Vers 300 avant JC : Livres VII à IX des Éléments d'Euclide
divisibilité, nombres premiers, PGCD
- IIIe siècle après JC : Les Arithmétiques de Diophante
Résolution d'équations à coefficients dans $\mathbb{Z}$
- XVIIe siècle : Fermat
 - Petit théorème de Fermat : $a^p \equiv a \pmod{p}$
 - Grand théorème de Fermat : $x^n + y^n = z^n$
 - Nombres de Fermat : $F_n = 2^{2^n} + 1$

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones

- Vers 300 avant JC : Livres VII à IX des Éléments d'Euclide
divisibilité, nombres premiers, PGCD
- IIIe siècle après JC : Les Arithmétiques de Diophante
Résolution d'équations à coefficients dans $\mathbb{Z}$
- XVIIe siècle : Fermat
 - Petit théorème de Fermat : $a^p \equiv a \pmod{p}$
 - Grand théorème de Fermat : $x^n + y^n = z^n$
 - Nombres de Fermat : $F_n = 2^{2^n} + 1$
 - Équation de Pell-Fermat : $x^2 - dy^2 = m$

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones

- Vers 300 avant JC : Livres VII à IX des Éléments d'Euclide
divisibilité, nombres premiers, PGCD
- IIIe siècle après JC : Les Arithmétiques de Diophante
Résolution d'équations à coefficients dans $\mathbb{Z}$
- XVIIe siècle : Fermat
 - Petit théorème de Fermat : $a^p \equiv a \pmod{p}$
 - Grand théorème de Fermat : $x^n + y^n = z^n$
 - Nombres de Fermat : $F_n = 2^{2^n} + 1$
 - Équation de Pell-Fermat : $x^2 - dy^2 = m$
 - Théorème des deux carrés : $p = a^2 + b^2 \Leftrightarrow p = 4k + 1$

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones au XVIIIe

- Euler

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones au XVIIIe

- Euler
 - Démonstre et généralise le petit théorème de Fermat

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones au XVIIIe

- Euler
 - Démontre et généralise le petit théorème de Fermat
 - Lien entre nombre premiers et fonction zêta de Riemann

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones au XVIIIe

- Euler
 - Démontre et généralise le petit théorème de Fermat
 - Lien entre nombre premiers et fonction zêta de Riemann
 - Preuve du théorème des deux carrés et travaille sur les quatre carrés

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones au XVIIIe

- Euler
 - Démontre et généralise le petit théorème de Fermat
 - Lien entre nombre premiers et fonction zêta de Riemann
 - Preuve du théorème des deux carrés et travaille sur les quatre carrés
 - Démontre que $F_5 = 2^{2^5} + 1$ n'est pas premier et $2^{31} - 1$ est un nombre de Mersenne premier

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones au XVIIIe

- Euler
 - Démontre et généralise le petit théorème de Fermat
 - Lien entre nombre premiers et fonction zêta de Riemann
 - Preuve du théorème des deux carrés et travaille sur les quatre carrés
 - Démontre que $F_5 = 2^{2^5} + 1$ n'est pas premier et $2^{31} - 1$ est un nombre de Mersenne premier
 - Conjecture la loi de réciprocité quadratique

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones au XVIIIe

- Lagrange

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones au XVIIIe

- Lagrange
 - Théorème des quatre carrés

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones au XVIIIe

- Lagrange
 - Théorème des quatre carrés
 - Initie la théorie des formes quadratiques

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones au XVIIIe

- Lagrange
 - Théorème des quatre carrés
 - Initie la théorie des formes quadratiques
 - Démontre le théorème de Wilson $(p-1)! \equiv -1 \pmod{p}$

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones au XVIIIe

- Lagrange
 - Théorème des quatre carrés
 - Initie la théorie des formes quadratiques
 - Démontre le théorème de Wilson $(p-1)! \equiv -1 \pmod{p}$
- Legendre

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones au XVIIIe

- Lagrange
 - Théorème des quatre carrés
 - Initie la théorie des formes quadratiques
 - Démontre le théorème de Wilson $(p-1)! \equiv -1 \pmod{p}$
- Legendre
 - Preuve incomplète de la loi de réciprocité quadratique

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones au XVIIIe

- Lagrange
 - Théorème des quatre carrés
 - Initie la théorie des formes quadratiques
 - Démontre le théorème de Wilson $(p-1)! \equiv -1 \pmod{p}$
- Legendre
 - Preuve incomplète de la loi de réciprocité quadratique
 - Introduction du symbole de Legendre

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones au XVIIIe

- Lagrange
 - Théorème des quatre carrés
 - Initie la théorie des formes quadratiques
 - Démontre le théorème de Wilson $(p-1)! \equiv -1 \pmod{p}$
- Legendre
 - Preuve incomplète de la loi de réciprocité quadratique
 - Introduction du symbole de Legendre
 - Conjecture le théorème des nombres premiers en 1797-1798

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones au XVIIIe

- Lagrange
 - Théorème des quatre carrés
 - Initie la théorie des formes quadratiques
 - Démontre le théorème de Wilson $(p-1)! \equiv -1 \pmod{p}$
- Legendre
 - Preuve incomplète de la loi de réciprocité quadratique
 - Introduction du symbole de Legendre
 - Conjecture le théorème des nombres premiers en 1797-1798
 - Gauss le conjecture en 1792-1793 à 15 ou 16 ans à la marge d'une table de logarithmes

Le contexte des Disquisitiones

L'arithmétique avant les Disquisitiones au XVIIIe



Figure: Euler - Lagrange - Legendre

Le contenu des Disquisitiones

L'édition de 1801

- Imprimé à Leipzig en 1801

Le contenu des Disquisitiones

L'édition de 1801

- Imprimé à Leipzig en 1801
- Rédigé en latin, traduit en français en 1807 par Pouillet-Deslisle

Le contenu des Disquisitiones

L'édition de 1801

- Imprimé à Leipzig en 1801
- Rédigé en latin, traduit en français en 1807 par Pouillet-Deslisle
- Comporte 7 sections et 366 articles

Le contenu des Disquisitiones

L'édition de 1801

- Imprimé à Leipzig en 1801
- Rédigé en latin, traduit en français en 1807 par Pouillet-Deslisle
- Comporte 7 sections et 366 articles
- Style très aride mais va à l'essentiel cherchant la généralité

Le contenu des Disquisitiones

L'édition de 1801

- Imprimé à Leipzig en 1801
- Rédigé en latin, traduit en français en 1807 par Pouillet-Deslisle
- Comporte 7 sections et 366 articles
- Style très aride mais va à l'essentiel cherchant la généralité
- Les sections 1 à 4 rédigées dès 1796

Le contenu des Disquisitiones

L'édition de 1801

- Imprimé à Leipzig en 1801
- Rédigé en latin, traduit en français en 1807 par Pouillet-Deslisle
- Comporte 7 sections et 366 articles
- Style très aride mais va à l'essentiel cherchant la généralité
- Les sections 1 à 4 rédigées dès 1796
- Existence d'une section 8 retirée pour baisser les coûts

Le contenu des Disquisitiones

L'épître dédicatoire au Duc de Brunswick

Par vos seules bontés, libre des soins étrangers, et maître de consacrer mon temps à l'étude, j'ai pu entreprendre les recherches dont cet Ouvrage renferme une partie, et m'y livrer pendant plusieurs années. Lorsque j'ai désiré de le mettre au jour, votre munificence a écarté tous les obstacles qui en retardaient la publication. Il m'est plus facile de

Le contenu des Disquisitiones

L'épître dédicatoire au Duc de Brunswick

- Remerciements pour le laisser libre de faire ses recherches

Le contenu des Disquisitiones

L'épître dédicatoire au Duc de Brunswick

- Remerciements pour le laisser libre de faire ses recherches
- Rappel sur sa « libéralité » à l'égard de ceux qui font des sciences

Le contenu des Disquisitiones

La préface

- Rappel de ce qu'est l'arithmétique « où l'on considère particulièrement les nombres entiers »

Le contenu des Disquisitiones

La préface

- Rappel de ce qu'est l'arithmétique « où l'on considère particulièrement les nombres entiers »
- Hommage aux « modernes »

couvertes. La Science est bien plus redevable aux modernes, parmi lesquels peu d'hommes à la vérité, mais tous dignes d'une gloire immortelle, FERMAT, EULER, LAGRANGE, LEGENDRE (et un petit nombre d'autres), ont ouvert l'entrée de cette science divine, et ont découvert la mine inépuisable de richesses qu'elle renferme. Je n'entre pas

Le contenu des Disquisitiones

La préface

- Explique qu'en 1795 il n'avait pas connaissance de ce qui avait été fait

Le contenu des Disquisitiones

La préface

- Explique qu'en 1795 il n'avait pas connaissance de ce qui avait été fait
- Prend connaissance du livre de Legendre qu'une fois la publication lancée

Le contenu des Disquisitiones

La préface

- Explique qu'en 1795 il n'avait pas connaissance de ce qui avait été fait
- Prend connaissance du livre de Legendre qu'une fois la publication lancée
- Explique section VII pas purement arithmétique

Le contenu des Disquisitiones

Les sections

- Les sections I à III forment un long prolégomène

Le contenu des Disquisitiones

Les sections

- Les sections I à III forment un long prolégomène
- Gauss ordonne des résultats déjà connus mais dispersés

Le contenu des Disquisitiones

Les sections

- Les sections I à III forment un long prolégomène
- Gauss ordonne des résultats déjà connus mais dispersés
- Il les dote d'une certaine cohésion en donnant des démonstrations générales

Le contenu des Disquisitiones

Les sections

- Les sections I à III forment un long prolégomène
- Gauss ordonne des résultats déjà connus mais dispersés
- Il les dote d'une certaine cohésion en donnant des démonstrations générales
- Les sections IV à VI forment le cœur des recherches

Le contenu des Disquisitiones

Les sections

- Les sections I à III forment un long prolégomène
- Gauss ordonne des résultats déjà connus mais dispersés
- Il les dote d'une certaine cohésion en donnant des démonstrations générales
- Les sections IV à VI forment le cœur des recherches
- Il y a de nombreuses contributions originales

Le contenu des Disquisitiones

Les sections

- Les sections I à III forment un long prolégomène
- Gauss ordonne des résultats déjà connus mais dispersés
- Il les dote d'une certaine cohésion en donnant des démonstrations générales
- Les sections IV à VI forment le cœur des recherches
- Il y a de nombreuses contributions originales
- La section VII porte sur la cyclotomie et la construction des polygones réguliers à la règle et au compas

Le contenu des Disquisitiones

La section I

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

Le contenu des Disquisitiones

La section I

- Gauss introduit la congruence

Le contenu des Disquisitiones

La section I

- Gauss introduit la congruence
- $a \equiv b [n]$ si n divise $a - b$

Le contenu des Disquisitiones

La section I

- Gauss introduit la congruence
- $a \equiv b [n]$ si n divise $a - b$
- Il démontre la compatibilité avec l'addition, le produit, etc...

Le contenu des Disquisitiones

Les sections II et III

- Il étudie les congruences de degré 1

Le contenu des Disquisitiones

Les sections II et III

- Il étudie les congruences de degré 1
- On y trouve tous les classiques de l'arithmétique :

Le contenu des Disquisitiones

Les sections II et III

- Il étudie les congruences de degré 1
- On y trouve tous les classiques de l'arithmétique :
- PGCD, nombres premiers, restes chinois, petit théorème de Fermat, théorème d'Euler, indicatrice d'Euler, théorème de Wilson, etc..

Le contenu des Disquisitiones

La section IV

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.

Le contenu des Disquisitiones

La section IV

- La loi de réciprocité quadratique provient de l'étude des équations de degré 2 modulo p

Le contenu des Disquisitiones

La section IV

- La loi de réciprocité quadratique provient de l'étude des équations de degré 2 modulo p
- On dit que $a \in \mathbb{Z}$ est un *résidu quadratique* modulo p (un nombre premier) s'il existe $m \in \mathbb{Z}$ tel que :

$$m^2 \equiv a [p] .$$

Le contenu des Disquisitiones

La section IV

- La loi de réciprocité quadratique provient de l'étude des équations de degré 2 modulo p
- On dit que $a \in \mathbb{Z}$ est un *résidu quadratique* modulo p (un nombre premier) s'il existe $m \in \mathbb{Z}$ tel que :

$$m^2 \equiv a [p] .$$

- Introduisons le *symbole de Legendre* :

$$\left(\frac{p}{q}\right) = \begin{cases} 1 & \text{si } p \text{ est un résidu quadratique modulo } q \\ -1 & \text{si } p \text{ n'est pas un résidu quadratique modulo } q \end{cases}$$

Le contenu des Disquisitiones

La section IV

- Loi de réciprocité quadratique : si p, q sont deux nombres premiers impairs alors :

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$$

Le contenu des Disquisitiones

La section IV

- Loi de réciprocité quadratique : si p, q sont deux nombres premiers impairs alors :

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$$

- Les lois complémentaires :

Le contenu des Disquisitiones

La section IV

- Loi de réciprocité quadratique : si p, q sont deux nombres premiers impairs alors :

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$$

- Les lois complémentaires :

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Le contenu des Disquisitiones

La section IV

- Loi de réciprocité quadratique : si p, q sont deux nombres premiers impairs alors :

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$$

- Les lois complémentaires :

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Le contenu des Disquisitiones

La section IV

- Algorithme efficace pour savoir si un nombre est un carré modulo p

Le contenu des Disquisitiones

La section IV

- Algorithme efficace pour savoir si un nombre est un carré modulo p
- Permet de savoir si une équation de degré 2 possède une solution modulo p

Le contenu des Disquisitiones

La section IV

- Algorithme efficace pour savoir si un nombre est un carré modulo p
- Permet de savoir si une équation de degré 2 possède une solution modulo p
- Compte le nombre de solutions de l'équation $x^2 \equiv p \pmod{q}$ car :

$$\text{Card} \left(\{x \in \mathbb{F}_q \mid x^2 = p\} \right) = 1 + \left(\frac{p}{q} \right)$$

Le contenu des Disquisitiones

Les sections V et VI

- Gauss étudie les formes quadratiques binaires entières :

$$Q(x, y) = ax^2 + bxy + cy^2, \quad a, b, c \in \mathbb{Z}$$

où le discriminant est $b^2 - 4ac$.

Le contenu des Disquisitiones

Les sections V et VI

- Gauss étudie les formes quadratiques binaires entières :

$$Q(x, y) = ax^2 + bxy + cy^2, \quad a, b, c \in \mathbb{Z}$$

où le discriminant est $b^2 - 4ac$.

- Il cherche à savoir quand est-ce qu'une forme Q représente un entier n c'est-à-dire :

$$\exists x, y \in \mathbb{Z}, \quad n = Q(x, y)$$

Le contenu des Disquisitiones

La section V et VI

- Permet de développer un nouvel outil pour résoudre des équations diophantiennes

Le contenu des Disquisitiones

La section V et VI

- Permet de développer un nouvel outil pour résoudre des équations diophantiennes
- $Q(x, y) = x^2 + y^2$ théorème des deux carrés

Le contenu des Disquisitiones

La section V et VI

- Permet de développer un nouvel outil pour résoudre des équations diophantiennes
- $Q(x, y) = x^2 + y^2$ théorème des deux carrés
- $Q(x, y) = x^2 - dy^2$ équation de Pell-Fermat

Le contenu des Disquisitiones

La section V et VI

- Gauss étudie l'action des matrices 2×2 sur $\mathbb{Z}$ de déterminant ± 1 (noté $GL_2(\mathbb{Z})$)

Le contenu des Disquisitiones

La section V et VI

- Gauss étudie l'action des matrices 2×2 sur $\mathbb{Z}$ de déterminant ± 1 (noté $GL_2(\mathbb{Z})$)
- Il découvre une loi de composition sur les classes d'équivalence sous l'action de $SL_2(\mathbb{Z})$ (déterminant 1) des formes quadratiques binaires entières de discriminant donné D

Le contenu des Disquisitiones

La section V et VI

- Gauss étudie l'action des matrices 2×2 sur $\mathbb{Z}$ de déterminant ± 1 (noté $GL_2(\mathbb{Z})$)
- Il découvre une loi de composition sur les classes d'équivalence sous l'action de $SL_2(\mathbb{Z})$ (déterminant 1) des formes quadratiques binaires entières de discriminant donné D
- Cela crée un groupe abélien fini qui permet de comprendre les corps quadratiques $\mathbb{Q}(\sqrt{D})$

Le contenu des Disquisitiones

La section VII

Cependant aucune de ces équations n'est si commode à traiter, ni se prête tant à notre dessein, que l'équation $x^n - 1 = 0$, dont on sait que les racines sont intimement liées avec les racines des premières. En effet, si l'on représente par i la quantité imaginaire $\sqrt{-1}$, les racines de l'équation $x^n - 1 = 0$ sont représentées par la formule

$$\cos \frac{KP}{n} + i \sin \frac{KP}{n} = r,$$

où l'on doit prendre pour K tous les nombres $1, 2, 3, \dots, n-1$;

Le contenu des Disquisitiones

La section VII

- Gauss étudie l'équation $X^n - 1 = 0$ sur $\mathbb{C}$

Le contenu des Disquisitiones

La section VII

- Gauss étudie l'équation $X^n - 1 = 0$ sur $\mathbb{C}$
- Les solutions sont de la forme $e^{\frac{2k\pi}{n}i}$ pour $0 \leq k \leq n-1$

Le contenu des Disquisitiones

La section VII

- Gauss étudie l'équation $X^n - 1 = 0$ sur $\mathbb{C}$
- Les solutions sont de la forme $e^{\frac{2k\pi}{n}i}$ pour $0 \leq k \leq n - 1$
- Il introduit les polynômes cyclotomiques et montre la structure cyclique de leurs racines

Le contenu des Disquisitiones

La section VII

- Gauss étudie l'équation $X^n - 1 = 0$ sur $\mathbb{C}$
- Les solutions sont de la forme $e^{\frac{2k\pi}{n}i}$ pour $0 \leq k \leq n - 1$
- Il introduit les polynômes cyclotomiques et montre la structure cyclique de leurs racines
- Il étudie l'action du groupe de Galois sur ces racines

Le contenu des Disquisitiones

La section VII

- Gauss étudie l'équation $X^n - 1 = 0$ sur $\mathbb{C}$
- Les solutions sont de la forme $e^{\frac{2k\pi}{n}i}$ pour $0 \leq k \leq n-1$
- Il introduit les polynômes cyclotomiques et montre la structure cyclique de leurs racines
- Il étudie l'action du groupe de Galois sur ces racines
- Il donne une méthode pour calculer ces racines

Le contenu des Disquisitiones

La section VII

- Gauss applique cette étude à la construction des polygones réguliers à la règle et au compas

Le contenu des Disquisitiones

La section VII

- Gauss applique cette étude à la construction des polygones réguliers à la règle et au compas
- Le polygone P_n est constructible si et seulement si n est une puissance de 2 ou un produit d'une puissance de 2 et d'un produit de nombres premiers de Fermat $F_k = 2^{2^k} + 1$

Le contenu des Disquisitiones

La section VII

- Gauss applique cette étude à la construction des polygones réguliers à la règle et au compas
- Le polygone P_n est constructible si et seulement si n est une puissance de 2 ou un produit d'une puissance de 2 et d'un produit de nombres premiers de Fermat $F_k = 2^{2^k} + 1$
- P_5 , P_{17} , P_{257} sont constructibles mais P_7 ne l'est pas

Postérité des Disquisitiones

Les congruences et la cyclotomie

- Les notions de congruences et de racines de l'unité ont permis de dégager les notions de groupe, d'anneau et de corps

Postérité des Disquisitiones

Les congruences et la cyclotomie

- Les notions de congruences et de racines de l'unité ont permis de dégager les notions de groupe, d'anneau et de corps
- Les permutations de racines de l'unité et la constructibilité des polygones sont une prémisse à la théorie de Galois

Postérité des Disquisitiones

Les congruences et la cyclotomie

- Les notions de congruences et de racines de l'unité ont permis de dégager les notions de groupe, d'anneau et de corps
- Les permutations de racines de l'unité et la constructibilité des polygones sont une prémisse à la théorie de Galois
- On a également développé les corps cyclotomiques $\mathbb{Q}(\zeta)$ où ζ est une racine de l'unité

Postérité des Disquisitiones

Les congruences et la cyclotomie

- Les notions de congruences et de racines de l'unité ont permis de dégager les notions de groupe, d'anneau et de corps
- Les permutations de racines de l'unité et la constructibilité des polygones sont une prémisse à la théorie de Galois
- On a également développé les corps cyclotomiques $\mathbb{Q}(\zeta)$ où ζ est une racine de l'unité
- Ces corps ont permis des avancées dans la démonstration du théorème de Fermat (théorie de Kummer)

Postérité des Disquisitiones

La loi de réciprocité quadratique

- Nombreuses démonstrations et généralisations

Postérité des Disquisitiones

La loi de réciprocité quadratique

- Nombreuses démonstrations et généralisations
- Permet de démontrer si un polynôme peut totalement se décomposer modulo p

Postérité des Disquisitiones

La loi de réciprocité quadratique

- Nombreuses démonstrations et généralisations
- Permet de démontrer si un polynôme peut totalement se décomposer modulo p
- Peut se généraliser en la réciprocité d'Artin :

$$C_K / N_{L|K}(C_L) \simeq \text{Gal}(L | K)^{\text{ab}}$$

Postérité des Disquisitiones

La loi de réciprocité quadratique

- Nombreuses démonstrations et généralisations
- Permet de démontrer si un polynôme peut totalement se décomposer modulo p
- Peut se généraliser en la réciprocité d'Artin :

$$C_K / N_{L|K}(C_L) \simeq \text{Gal}(L | K)^{\text{ab}}$$

- Certains ensembles ne possèdent pas la propriété de factorialité, cette réciprocité permet de savoir lorsque des idéaux sont décomposables

Postérité des Disquisitiones

La loi de réciprocité quadratique

- Nombreuses démonstrations et généralisations
- Permet de démontrer si un polynôme peut totalement se décomposer modulo p
- Peut se généraliser en la réciprocité d'Artin :

$$C_K / N_{L|K}(C_L) \simeq \text{Gal}(L|K)^{\text{ab}}$$

- Certains ensembles ne possèdent pas la propriété de factorialité, cette réciprocité permet de savoir lorsque des idéaux sont décomposables
- C'est la théorie du corps de classe

Postérité des Disquisitiones

La loi de réciprocité quadratique

- La théorie du corps de classe répond (partiellement) au neuvième problème de Hilbert : établir une loi de réciprocité quadratique dans les corps de nombres

Postérité des Disquisitiones

La loi de réciprocité quadratique

- La théorie du corps de classe répond (partiellement) au neuvième problème de Hilbert : établir une loi de réciprocité quadratique dans les corps de nombres
- Ce problème est toujours ouvert dans le cas non-abélien (galoisien) et dans le cas non-galoisien

Postérité des Disquisitiones

La loi de réciprocité quadratique

- La théorie du corps de classe répond (partiellement) au neuvième problème de Hilbert : établir une loi de réciprocité quadratique dans les corps de nombres
- Ce problème est toujours ouvert dans le cas non-abélien (galoisien) et dans le cas non-galoisien
- C'est un des sujets principaux du Programme de Langlands

Postérité des Disquisitiones

La loi de réciprocité quadratique

- Le théorème de réciprocité de Artin est équivalent au théorème de Kronecker-Weber qui dit que toute extension abélienne finie de $\mathbb{Q}$ est incluse dans une extension cyclotomique

Postérité des Disquisitiones

La loi de réciprocité quadratique

- Le théorème de réciprocité de Artin est équivalent au théorème de Kronecker-Weber qui dit que toute extension abélienne finie de $\mathbb{Q}$ est incluse dans une extension cyclotomique
- Gauss avait donc bien compris le lien entre cyclotomie et réciprocité quadratique !

Postérité des Disquisitiones

La loi de réciprocité quadratique

- Enfin la réciprocité quadratique permet de compter le nombre de solutions de certaines équations modulo p

Postérité des Disquisitiones

La loi de réciprocité quadratique

- Enfin la réciprocité quadratique permet de compter le nombre de solutions de certaines équations modulo p
- Ces objets deviendront plus tard des variétés algébriques sur des corps finis pour lesquelles on peut compter le nombre de points

Postérité des Disquisitiones

La loi de réciprocité quadratique

- Enfin la réciprocité quadratique permet de compter le nombre de solutions de certaines équations modulo p
- Ces objets deviendront plus tard des variétés algébriques sur des corps finis pour lesquelles on peut compter le nombre de points
- Ce sont donc les prémisses des conjectures de Weil qui guideront le développement de la géométrie algébrique moderne

Postérité des Disquisitiones

Composition des formes binaires quadratiques entières

- Manjul Bhargava, dans sa thèse soutenue en 2001, généralisa la loi de composition de Gauss sur les formes quadratiques

Postérité des Disquisitiones

Composition des formes binaires quadratiques entières

- Manjul Bhargava, dans sa thèse soutenue en 2001, généralisa la loi de composition de Gauss sur les formes quadratiques
- En observant un Rubik's Cube $2 \times 2 \times 2$, il comprit comment simplifier et généraliser les travaux de Gauss

Postérité des Disquisitiones

Composition des formes binaires quadratiques entières

- Manjul Bhargava, dans sa thèse soutenue en 2001, généralisa la loi de composition de Gauss sur les formes quadratiques
- En observant un Rubik's Cube $2 \times 2 \times 2$, il comprit comment simplifier et généraliser les travaux de Gauss
- Il obtint le prix Fermat en 2011 et la médaille Fields en 2014



MERCI!