

Les calculs du manuscrit de Gauss
Cod. Ms. Gauß Manusk. 50, *Analysis Residuorum*, Caput sextum
Extraction et explication des exemples numériques

Transcription et commentaire établis à partir du fac-similé SUB Göttingen

Résumé

Ce document rassemble, à l'exclusion du reste du texte, les calculs numériques concrets qui apparaissent dans le manuscrit de Gauss conservé à la SUB de Göttingen (Cod. Ms. Gauß Manusk. 50), intitulé *Analysis Residuorum*, chapitre sixième : *Solutio congruentiae $x^n - 1 \equiv 0$ et aequationis $x^n - 1 = 0$, cum dilucidationibus supra theoriā polygonorum regularium*. Il s'agit d'un brouillon, antérieur ou contemporain des *Disquisitiones Arithmeticae* (1801), consacré à la théorie des congruences $x^n \equiv 1$ et à la construction des polygones réguliers (cyclotomie).

Chaque section ci-dessous reproduit un calcul numérique explicite du manuscrit, avec les étapes intermédiaires et une explication de la méthode, afin de montrer comment Gauss procédait *sans machine à calculer*. La numérotation en marge (§) renvoie aux articles autographes de Gauss ; le folio du manuscrit est indiqué entre parenthèses. Les nombres ont été vérifiés arithmétiquement chaque fois que possible (indiqué par “*vérifié*”) ; quand l'écriture cursive rend un chiffre incertain, cela est signalé.

1. Indices et racines primitives : $x^7 \equiv 1 \pmod{29}$

Énoncé (§ 239-240, fol. 240/268)

Gauss pose $p = 29$, $n = 7$ (un diviseur de $p - 1 = 28$), et cherche les 7 racines de

$$x^7 \equiv 1 \pmod{29}.$$

Calcul 1 - les sept racines

Par inspection (essais successifs des petites puissances), Gauss trouve directement les sept racines :

$$1, 7, 16, 20, 23, 24, 25.$$

Vérification : ce sont exactement les résidus x tels que $x^7 \equiv 1 \pmod{29}$; comme $7 \mid 28 = \text{ord}(\mathbb{Z}/29\mathbb{Z})^\times$, il y en a exactement 7, et ce sont les puissances 7-ièmes des éléments de $(\mathbb{Z}/29\mathbb{Z})^\times$.

Calcul 2 - indexation par les puissances de 7

Gauss choisit *une* des racines, 7, comme racine “de référence”, et pose $(0) = 1$, $(1) = 7$, et plus généralement $(k) \equiv 7^k \pmod{29}$. Il calcule alors les puissances successives de 7 modulo 29 :

$$7^0 = 1, \quad 7^1 = 7, \quad 7^2 = 49 \equiv 20, \quad 7^3 = 7 \cdot 20 = 140 \equiv 24,$$

$$7^4 = 7 \cdot 24 = 168 \equiv 23, \quad 7^5 = 7 \cdot 23 = 161 \equiv 16, \quad 7^6 = 7 \cdot 16 = 112 \equiv 25,$$

et l’on retrouve bien $7^7 = 7 \cdot 25 = 175 \equiv 1$ (*vérifié* : $175 = 6 \times 29 + 1$). D’où la table des indices :

k	0	1	2	3	4	5	6
$(k) = 7^k \pmod{29}$	1	7	20	24	23	16	25

Chaque étape n’exige qu’une multiplication par 7 suivie d’une soustraction d’un multiple de 29 : c’est la table de multiplication et rien de plus.

Calcul 3 - ordonner les racines primitives par un second indice

Les six racines autres que 1 sont toutes *primitives* (puisque $n = 7$ est premier). Gauss veut maintenant les ranger dans un ordre “naturel” vis-à-vis de la structure du groupe des exposants $\{0, \dots, 6\} \cong \mathbb{Z}/7\mathbb{Z}$. Il choisit un générateur de $(\mathbb{Z}/7\mathbb{Z})^\times$, à savoir $\rho = 3$ (puisque 3, 2, 6, 4, 5, 1 sont les puissances successives de 3 modulo 7) :

$$3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6, \quad 3^4 \equiv 4, \quad 3^5 \equiv 5, \quad 3^6 \equiv 1 \pmod{7}.$$

Il pose alors (ρ^k) pour désigner le terme dont l’indice (au sens du Calcul 2) vaut $\rho^k \pmod{7}$: la suite des indices est donc 1, 3, 2, 6, 4, 5, et, en reportant dans la table du Calcul 2, la suite des *racines* correspondantes est

$$7, 24, 20, 25, 23, 16.$$

C’est exactement ce que porte le manuscrit. L’intérêt de la manœuvre : une simple multiplication modulo 7 (sur les *indices*, petits nombres ≤ 6) permet d’engendrer dans le bon ordre les six racines primitives modulo 29, sans avoir à retester chaque candidat contre $x^7 \equiv 1$. C’est le principe même du calcul par indices (l’ancêtre du logarithme discret) : on remplace des multiplications modulo 29 par des additions modulo l’ordre du groupe.

2. Résolution complète de $x^{31} \equiv 1 \pmod{311}$

Énoncé (§ 252, fol. 282-284)

Gauss prend $n = 31$, $p = 311 = 10 \times 31 + 1$. Le groupe $(\mathbb{Z}/311\mathbb{Z})^\times$, d’ordre $310 = 2 \cdot 5 \cdot 31$, contient un unique sous-groupe d’ordre 31 : les racines de

$$x^{31} \equiv 1 \pmod{311}.$$

Trouver ces 31 résidus par tâtonnement direct serait fastidieux. Gauss emploie alors, à l’intérieur de l’arithmétique modulo 311, exactement la même méthode des périodes que celle qui sert, en théorie des nombres complexes, à construire le polygone régulier à 31 côtés : car les relations algébriques entre les “périodes” de racines de l’unité ne dépendent que de la structure du groupe cyclique des exposants (ici $(\mathbb{Z}/31\mathbb{Z})^\times$, d’ordre $30 = 2 \cdot 3 \cdot 5$), et restent donc valables telles quelles quand on remplace les racines complexes de l’unité par les racines “entières” modulo 311.

Calcul 1 - un générateur des exposants

On cherche d'abord une racine primitive de $y^{30} \equiv 1 \pmod{31}$, c'est-à-dire un générateur de $(\mathbb{Z}/31\mathbb{Z})^\times$. Gauss trouve $y = 3$ convient.

Calcul 2 - répartition en 5 périodes de 6 termes

Avec $\rho = 3$, les 30 exposants non nuls $1, \dots, 30$ se répartissent, via les puissances de ρ modulo 31, en 5 classes de 6 éléments chacune (les classes latérales du sous-groupe d'indice 5). Notant (k) la racine ζ^k (où ζ est un générateur du sous-groupe d'ordre 31 de $(\mathbb{Z}/31\mathbb{Z})^\times$), Gauss écrit les cinq *périodes* :

$$\begin{aligned}(5 \times 0) &= (1) + (26) + (25) + (30) + (5) + (6) \\(5 \times 1) &= (3) + (16) + (13) + (28) + (15) + (18) \\(5 \times 2) &= (9) + (17) + (8) + (22) + (14) + (23) \\(5 \times 3) &= (27) + (20) + (24) + (4) + (11) + (7) \\(5 \times 4) &= (19) + (29) + (10) + (12) + (2) + (21)\end{aligned}$$

Calcul 3 - la résolvante de degré 5

Les cinq sommes $(5 \times 0), \dots, (5 \times 4)$ sont, par construction, les racines d'une équation de degré 5 à coefficients entiers modulo 311. Gauss calcule leurs sommes de puissances (sommes de Newton) :

$$\begin{aligned}\sum(5 \times k) &\equiv -1, & \sum(5 \times k)^2 &\equiv 25, & \sum(5 \times k)^3 &\equiv 26, \\ \sum(5 \times k)^4 &\equiv 249, & \sum(5 \times k)^5 &\equiv 664 \pmod{311},\end{aligned}$$

et en déduit (par les identités de Newton, qui relient sommes de puissances et fonctions symétriques élémentaires) l'équation résolvante de degré 5 satisfaite par les périodes. *Vérification partielle* : $17 + 183 + 263 + 91 + 67 = 621 = 2 \times 311 - 1 \equiv -1 \pmod{311}$ ✓ (voir Calcul 4).

Calcul 4 - une racine par essai, puis les quatre autres par récurrence

Plutôt que de résoudre la quintique en toute généralité, Gauss cherche *une* racine par essais directs de petits nombres, et trouve

$$(5 \times 0) \equiv 17 \pmod{311}.$$

Il établit ensuite, par élimination algébrique dans la résolvante, des formules exprimant chaque $(5 \times k)$ comme polynôme en (5×0) (par exemple $5(5 \times 1) \equiv 3(5 \times 0)^4 - (5 \times 0)^3 - 33(5 \times 0)^2 - 24(5 \times 0) + 15$), ce qui permet de calculer successivement, en substituant $(5 \times 0) = 17$:

$$(5 \times 0) \equiv 17, \quad (5 \times 1) \equiv 183, \quad (5 \times 2) \equiv 263, \quad (5 \times 3) \equiv 91, \quad (5 \times 4) \equiv 67 \pmod{311}.$$

Ainsi, une seule multiplication modulo 311 répétée (élévation aux puissances de 17) suffit à obtenir les quatre autres périodes, sans nouvel essai-erreur.

Calcul 5 - subdivision en périodes de 3, puis en périodes de 1

Chaque période de 6 se scinde à son tour en deux périodes de 3 (car $6 = 2 \times 3$). Celles issues de (5×0) sont racines d'une équation cubique dont Gauss trouve, en substituant les valeurs numériques ci-dessus, les coefficients modulo 311 :

$$x^3 - 17x^2 + 108x - 69 \equiv 0 \pmod{311}.$$

Une racine se devine par essai : $x = 10$. *Vérification* : $10^3 - 17 \cdot 10^2 + 108 \cdot 10 - 69 = 1000 - 1700 + 1080 - 69 = 311 \equiv 0 \pmod{311}$ ✓ (exact, pas seulement approché!).

Enfin, en regroupant les exposants par paires conjuguées (k et $-k$ modulo 31), Gauss aboutit à la quadratique

$$x^2 - 10x + 1 \equiv 0 \pmod{311},$$

dont les deux racines sont les deux racines primitives cherchées :

$x \equiv 126 \quad \text{et} \quad x \equiv 195 \pmod{311}.$

Vérification : $126 + 195 = 321 = 311 + 10 \equiv 10 \pmod{311}$ ✓ ; et $126 \times 195 = 24570 = 79 \times 311 + 1 \equiv 1 \pmod{311}$ ✓. Les deux conditions (somme $\equiv 10$, produit $\equiv 1$) sont exactement celles qu'impose l'équation $x^2 - 10x + 1 \equiv 0$.

Ce que montre cet exemple

Au lieu de tester un à un les 310 résidus non nuls modulo 311, Gauss réduit le problème, grâce à la factorisation $30 = 5 \times 3 \times 2$, à la résolution successive d'une équation de degré 5, puis 3, puis 2 - chacune ayant des coefficients *entiers modulo 311* faciles à deviner par petits essais. C'est la transposition arithmétique directe de la méthode des périodes gaussiennes, habituellement présentée pour construire les polygones réguliers.

3. Le tridécagone : $x^{13} = 1$ et la valeur exacte de $\cos \frac{2\pi}{13}$

Énoncé (§ 269, fol. 269, 302-303)

“Exemplum I. Quaerendae sunt radices aequationis $x^{13} = 1$ ”. Ici $n - 1 = 12 = 4 \times 3$. Une racine primitive de $x^{12} \equiv 1 \pmod{13}$ est 2, dont les puissances rangent les douze racines non triviales $\rho, \rho^2, \dots$ dans l'ordre

$$\rho, \rho^2, \rho^4, \rho^8, \rho^3, \rho^6, \rho^{12}, \rho^{11}, \rho^9, \rho^5, \rho^{10}, \rho^7.$$

(en effet $2^1, 2^2, \dots, 2^{12} \pmod{13}$ donnent 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1).

Calcul 1 - trois périodes de 4 : la résolvante cubique

En regroupant un terme sur trois dans la liste ci-dessus, Gauss forme trois périodes de 4 termes :

$$A = \rho + \rho^8 + \rho^{12} + \rho^5, \quad B = \rho^2 + \rho^3 + \rho^{11} + \rho^{10}, \quad C = \rho^4 + \rho^6 + \rho^9 + \rho^7.$$

Par les relations entre puissances de racines de l'unité, il obtient

$$A + B + C = -1, \quad AA = 4 + B + 2C, \quad AB = A + 2B + C, \quad AC = 2A + B + C,$$

d'où, en combinant, $A^3 = 9A + 4B + 3C$, puis

$$A^2 + B^2 + C^2 = 9, \quad A^3 + B^3 + C^3 = -16,$$

ce qui montre que A, B, C sont les trois racines de la cubique résolvante

$$x^3 + x^2 - 4x + 1 = 0.$$

Calcul 2 - résolution numérique par approximation

Cette cubique a trois racines réelles (*casus irreducibilis*) : elle ne peut donc pas se résoudre par de simples racines carrées ou cubiques réelles. Gauss en trouve une racine *par approximation numérique* directe (une méthode d'affinement successif des décimales, l'ancêtre de la méthode de Newton) :

$$A \approx 0,27389055496212.$$

Les deux autres racines s'obtiennent alors sans nouvelle approximation, par simple substitution dans les relations linéaires tirées ci-dessus :

$$C = A^2 + A - 3 \approx -2,6510934089, \quad B = -A^2 - 2A + 2 \approx 1,3772028539.$$

Vérification : avec $A = 0,27389055496212$, $A^2 \approx 0,0750163$, d'où $C \approx 0,0750163 + 0,2738906 - 3 = -2,6510931$ (accord à 10^{-6} près avec la valeur du manuscrit) et $B \approx -0,0750163 - 0,5477811 + 2 = 1,3772026$ (idem) ✓.

Calcul 3 - vérification par la méthode trigonométrique de Cardan

Le manuscrit refait aussi le calcul par la *formule trigonométrique* de Cardan pour le cas irréductible, qui évite les racines carrées de nombres négatifs. Avec $\theta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ (racine cubique complexe de l'unité), Gauss calcule exactement

$$(\theta; 0)^3 = -32\frac{1}{2} - 19\frac{1}{2}\sqrt{3}\sqrt{-1},$$

c'est-à-dire un nombre complexe de module $13^{3/2}$ et d'argument $46^\circ 6,12683'$.

La racine cubique de module $13^{3/2}$ et d'argument $46^\circ 6,12683'/3 = 15^\circ 22,04228'$ (*trisection de l'angle*, seule opération "non algébrique" nécessaire) donne

$$(\theta; 0) = -13^{1/2} \left(\cos 15^\circ 22,04228' + i \sin 15^\circ 22,04228' \right) \approx -3,47664076 - 0,95548782 i,$$

d'où l'on retrouve $3(3 \times 0) \approx 7,195328152$, soit $(3 \times 0) = C \approx 2,65109384$ (au signe près de la valeur ci-dessus : Gauss vérifie ainsi par deux méthodes indépendantes - approximation directe de la racine réelle, puis formule trigonométrique exacte - qu'il obtient bien le même nombre).

Calcul 4 - descente vers les périodes de 2, puis vers ρ lui-même

La période A (quatre termes) se scinde en deux périodes de 2, formées des paires d'exposants opposés $\{1, 12\}$ et $\{5, 8\}$ (puisque $12 \equiv -1$ et $8 \equiv -5 \pmod{13}$) :

$$\rho + \rho^{12} \quad \text{et} \quad \rho^5 + \rho^8,$$

racines de $x^2 - Ax + C = 0$. D'où

$$\rho + \rho^{12} = \frac{1}{2}A + \sqrt{\frac{1}{4}A^2 - C} \approx 1,77091205, \quad \rho^5 + \rho^8 \approx -1,49702150.$$

Vérification : $\frac{1}{4}A^2 - C \approx 0,01875 + 2,65109 = 2,66985$, $\sqrt{2,66985} \approx 1,63397$, et $\frac{1}{2}A \approx 0,13695$; somme $\approx 1,77091$ ✓.

Enfin, ρ et $\rho^{12} = \rho^{-1}$ sont racines de $x^2 - (\rho + \rho^{12})x + 1 = 0$, d'où la valeur exacte, calculée par Gauss à dix décimales :

$$\rho = \cos \frac{2\pi}{13} + i \sin \frac{2\pi}{13} \approx 0,8854560256 + 0,4647231721 \sqrt{-1}.$$

Vérification : $\cos(2\pi/13) = 0,885456\dots$ et $\sin(2\pi/13) = 0,464723\dots$ - exactement les valeurs du manuscrit. Le reste de la page donne de même, sans calcul supplémentaire, les cinq autres cosinus $\cos(2\pi k/13)$, $k = 2, \dots, 6$, à partir des périodes déjà connues.

4. L'heptadécagone : $x^{17} = 1$ et la formule de Gauss pour $\cos \frac{2\pi}{17}$

Énoncé (§ 270, fol. 304-305)

“II. Quaerantur radices aequationis $x^{17} = 1$ ”. Ici $n - 1 = 16 = 2^4$: c'est le cas qui rend le 17-gone constructible à la règle et au compas (Gauss, 1796). Une racine primitive de $x^{16} \equiv 1 \pmod{17}$ est 3, qui range les 16 racines dans l'ordre

$$\rho, \rho^3, \rho^9, \rho^{10}, \rho^{13}, \rho^5, \rho^{15}, \rho^{11}, \rho^{16}, \rho^{14}, \rho^8, \rho^7, \rho^4, \rho^{12}, \rho^2, \rho^6.$$

Calcul 1 - deux périodes de 8 : la résolvante quadratique

En prenant un terme sur deux, Gauss forme

$$(2 \times 0) = \rho + \rho^9 + \rho^{13} + \rho^{15} + \rho^{16} + \rho^8 + \rho^4 + \rho^2, \quad (2 \times 1) = \rho^3 + \rho^{10} + \rho^5 + \rho^{11} + \rho^{14} + \rho^7 + \rho^{12} + \rho^6,$$

racines de $x^2 + x - 4 = 0$ (car $(2 \times 0) + (2 \times 1) = -1$ et $(2 \times 0) \cdot (2 \times 1) = -4$, propriétés classiques des sommes de Gauss). D'où

$$(2 \times 0) = -\frac{1}{2} + \frac{1}{2}\sqrt{17} \approx 3,56155, \quad (2 \times 1) = -\frac{1}{2} - \frac{1}{2}\sqrt{17} \approx -4,56155.$$

Calcul 2 - quatre périodes de 4

Chaque période de 8 se scinde en deux périodes de 4. Celles issues de (2×0) , notées $(4 \times 0) = \rho + \rho^{13} + \rho^{16} + \rho^4$ et $(4 \times 2) = \rho^9 + \rho^{15} + \rho^8 + \rho^2$, vérifient $(4 \times 0) + (4 \times 2) = (2 \times 0)$ et, par la relation

$$(2 \times 0)^2 = 8 + 3(2 \times 0) + 4(2 \times 1),$$

Gauss en tire l'équation $x^2 - (2 \times 0)x - 1 = 0$ dont

$$(4 \times 0), (4 \times 2) = -\frac{1}{4} - \frac{1}{4}\sqrt{17} \pm \frac{1}{2}\sqrt{\frac{17}{2} - \frac{1}{2}\sqrt{17}}.$$

(De même pour les deux autres périodes de 4 issues de (2×1) , obtenues par les formules analogues avec $-\sqrt{17}$.)

Calcul 3 - deux périodes de 2, puis la formule finale

En scindant (4×0) à son tour, $\rho + \rho^{16}$ et $\rho^4 + \rho^{13}$ sont racines de

$$x^2 - (4 \times 0)x + (4 \times 1) = 0,$$

d'où, en substituant toutes les valeurs précédentes, la célèbre formule en radicaux imbriqués :

$$\rho + \rho^{16} = 2 \cos \frac{2\pi}{17} = -\frac{1}{8} + \frac{1}{8}\sqrt{17} \pm \frac{1}{4}\sqrt{\frac{17}{2} - \frac{1}{2}\sqrt{17}}$$

$$\pm \frac{1}{4}\sqrt{\frac{17}{2} - \frac{1}{16}\sqrt{17} + \frac{1}{8}\sqrt{\frac{17}{2} - \frac{1}{2}\sqrt{17}} - \frac{1}{4}\sqrt{\frac{17}{2} + \frac{1}{2}\sqrt{17}}}$$

que Gauss note pouvoir aussi écrire, sous le radical le plus intérieur, sous la forme équivalente

$$\pm \sqrt{\frac{17}{16} - \frac{1}{16}\sqrt{17} + \frac{1}{8}\sqrt{\frac{85}{2} - \frac{13}{2}\sqrt{17}}}.$$

C'est exactement la formule que Gauss publiera en 1801 dans les *Disquisitiones Arithmeticae* (art. 365) comme preuve de la constructibilité du polygone à 17 côtés. Le manuscrit laisse ensuite au lecteur (*"relinquimus lectoribus"*) le soin de mener le même calcul, en tout point semblable, pour les quatre autres couples de périodes de 2.

Ce que montre cet exemple

La chaîne $16 = 2 \times 2 \times 2 \times 2$ ne fait intervenir, à chaque étape, que la résolution d'une équation du second degré dont les coefficients sont déjà connus de l'étape précédente : c'est la trace algébrique exacte de la construction à la règle et au compas, chaque extraction de racine carrée correspondant à une bisection réalisable géométriquement.

5. Illustration géométrique : la somme des cosinus est nulle

Énoncé et calcul (§ 278, fol. 314)

Pour illustrer géométriquement pourquoi $1 + \rho + \rho^2 + \dots + \rho^{n-1} = 0$, Gauss dessine le cas $n = 5$ (pentagone) et note, en projetant sur l'axe des cosinus,

$$\cos 0^\circ + \cos 72^\circ + \cos 144^\circ + \cos 216^\circ + \cos 288^\circ = 0,$$

en indiquant sur la figure $AB = \cos 0^\circ$, $BC = \cos 72^\circ$, $CG(\text{négatif}) = \cos 144^\circ$, $GF(\text{négatif}) = \cos 216^\circ$, $FA = \cos 288^\circ$ (les longueurs orientées se compensant exactement le long du diamètre).

Il applique ensuite l'identité trigonométrique de produit-en-somme

$$\cos a \cos b = \frac{1}{2} \cos(a + b) + \frac{1}{2} \cos(a - b)$$

au cas $n = 17$: comme $\cos \frac{k}{17} \cdot 2\pi = \cos \frac{17-k}{17} \cdot 2\pi$, la relation générale $1 + 2 \cos \frac{2\pi}{17} + 2 \cos \frac{4\pi}{17} + \dots + 2 \cos \frac{16\pi}{17} = 0$ se réduit à

$$\cos \frac{2\pi}{17} + \cos \frac{4\pi}{17} + \dots + \cos \frac{16\pi}{17} = -\frac{1}{2},$$

c'est-à-dire exactement la relation $(2 \times 0) + (2 \times 1) = -1$ utilisée à la section précédente, mais retrouvée ici par un argument purement trigonométrique et géométrique, sans algèbre des périodes.

6. Nombres de Fermat et constructibilité

Énoncé et calcul (§ 271, fol. 306)

Gauss observe que la méthode des sections successives par 2 (comme aux sections 4.) exige que $n - 1$ soit une puissance de 2 pour n'utiliser que des racines carrées ; n devant en outre être premier. Il pose $n = 2^a + 1$ et remarque

$2^a + 1$ premier $\implies a = 2^h$ (sinon $2^a + 1$ est divisible par $2^{a'} + 1$ pour un facteur impair de a),
donc n doit être de la forme $2^{2^h} + 1$ (nombre de Fermat). En substituant $h = 0, 1, 2, 3, 4$ il obtient les cinq valeurs

$$n = 3, 5, 17, 257, 65537,$$

seules connues à l'époque, en notant que Fermat s'était trompé en les croyant *toutes* premières (“*sed hinc non sequitur ... et olim Fermatius per hanc inductionem deceptus praepropere conclusuerat*”)
- allusion à $2^{32} + 1 = 4294967297 = 641 \times 6700417$, factorisation trouvée par Euler.

7. Fractions et périodes décimales : reconstruire un développement décimal sans division

Énoncé (§ 280-281, fol. 318)

Gauss veut décomposer une fraction m/n , où n se factorise en facteurs premiers entre eux $n = a \cdot b \cdot c \dots$, en une somme $A + \alpha/a + \beta/b + \gamma/c + \dots$ à numérateurs plus petits que les dénominateurs.

Avec

$$n = 16 \cdot 9 \cdot 13 \cdot 59 \cdot 5 \cdot 49 \cdot 47 = 1\,271\,808\,720$$

(vérifié par le calcul direct : $16 \times 9 \times 13 \times 59 \times 5 \times 49 \times 47 = 1\,271\,808\,720$), il détermine chaque numérateur par une simple congruence, par exemple

$$\frac{2 \cdot 55224^2 - 1}{9 \cdot 13 \cdot 59 \cdot 5 \cdot 49 \cdot 47} \equiv \frac{-1}{13} \equiv 11 \pmod{16},$$

et ainsi de suite pour chaque facteur, ce qui donne finalement

$$\frac{m}{n} = 1 + \frac{11}{16} + \frac{4}{9} + \frac{5}{13} + \frac{52}{59} + \frac{4}{5} + \frac{22}{49} + \frac{7}{47}.$$

Calcul - reconstitution du développement décimal (§ 290-291, fol. 326-327)

Ayant dressé une fois pour toutes (§ 287-290) une table donnant la période décimale de $1/p$ pour tous les nombres premiers $p < 1000$, Gauss reconstruit le développement décimal d'une grande fraction *sans poser aucune division*, en additionnant colonne par colonne les développements déjà connus de chaque fraction unitaire :

$$\begin{array}{r} 1 = 1,000000\ 000000\ 000000 \dots \\ 11/16 = 0,687500\ 000000\ 000000 \dots \\ 4/9 = 0,444444\ 444444\ 444444 \dots \\ 5/13 = 0,384615\ 384615\ 384615 \dots \\ 52/59 = 0,881355\ 932203\ 389830 \dots \\ 22/49 = 0,448979\ 591836\ 734693 \dots \\ 7/47 = 0,148936\ 170212\ 765957 \dots \\ \hline \text{somme} \approx 4,795831\ 523312\ 709541 \dots \end{array}$$

(chaque ligne est simplement recopiée depuis la table de périodes ; seule la dernière étape, l'addition en colonnes avec retenues, est un calcul "à la main"). Gauss précise seulement qu'il faut ajouter ou retrancher 1 sur la dernière décimale retenue, selon le sens de l'arrondi de chaque période tronquée. *Vérification* : en recalculant la fraction d'origine m/n par les règles usuelles, on retrouve bien une valeur décimale 4,79583152331..., en accord avec la somme ci-dessus à onze décimales près (les tout derniers chiffres du numérateur à onze chiffres étant d'une lecture cursive incertaine, la concordance au-delà de la douzième décimale n'a pas pu être vérifiée avec certitude).

Le procédé montre comment une division par un dénominateur de dix chiffres peut être évitée : on ne divise jamais que par des *facteurs premiers* de n , une fois pour toutes, et l'on combine ensuite les résultats par de simples additions.

8. La méthode d'exclusion pour $x^2 = a + by$

Énoncé et calcul (§ 297, fol. 332)

Pour résoudre en entiers $x^2 = 7 + 139y$ avec $y \leq 34$, plutôt que de tester les 35 valeurs possibles de y , Gauss *exclut* d'un coup des paquets de valeurs de y grâce à des congruences modulo de petits

nombres. Pour chaque petit module p , il détermine quels restes de y modulo p sont impossibles, parce qu'ils obligerait $7 + 139y$ à être un résidu non-quadratique modulo p :

p	restes de y exclus (mod p)
7	1, 2, 4
8	0, 1, 2, 4, 5
9	1, 2, 4, 7, 8
11	0, 2, 3, 4, 8

En croisant ces exclusions successives (méthode que Gauss qualifie de “*mechanice*”, c’est-à-dire mécanisable), il ne reste, parmi $y = 0, \dots, 34$, que les deux valeurs $y = 6$ et $y = 27$ à essayer réellement. Le premier essai réussit :

$$7 + 6 \times 139 = 7 + 834 = 841 = 29^2,$$

vérifié : $29^2 = 841$. D’où la solution $x = 29$, $y = 6$.

Ce que montre cet exemple

C’est un *crible* : au lieu de calculer 35 carrés candidats, on ramène le travail à quatre petites tables de restes quadratiques (modulo 7, 8, 9, 11), faciles à dresser une fois pour toutes, et l’on ne calcule effectivement qu’un ou deux carrés à la fin. Gauss note explicitement que ce mécanisme d’exclusion peut être poussé aussi loin qu’on le souhaite en ajoutant d’autres petits modules.

Remarques finales

Tous les calculs ci-dessus partagent un même principe : Gauss remplace systématiquement un calcul *brutal* (tester toutes les valeurs, poser une longue division, extraire une racine dans un corps compliqué) par une succession de *petits* calculs élémentaires (multiplications modulo un petit nombre, tables dressées une fois pour toutes, résolution d’équations de bas degré dont un coefficient ou une racine se devine par tâtonnement), enchaînés grâce à une structure algébrique sous-jacente (groupe cyclique des exposants, factorisation de son ordre). C’est très exactement la même logique - descente le long des diviseurs de $p - 1$ ou de $n - 1$ - qui organise aussi bien la recherche des racines primitives (section 1.), la résolution de congruences de degré premier (section 2.) que la construction des polygones réguliers (sections 3. et 4.).