LES *DISQUISICIONS ARITMÈTIQUES* DE GAUSS

PILAR BAYER

RESUM. Aquest article presenta un apropament a l'obra *Disquisicions aritmètiques*, que C. F. Gauss publicà l'any 1801, quan comptava 24 anys. En una primera part, de caire històric, s'exposen les circumstàncies que van concórrer en la seva elaboració. En una segona part s'ofereix una visió del seu contingut, acompanyada d'algunes reflexions sobre la seva influència posterior.

Les *Disquisitiones Arithmeticæ* són una obra de joventut. Gauss ens diu que el seu contingut pertany a l'aritmètica superior, entesa com l'estudi dels nombres enters i, per extensió, dels nombres fraccionaris. Així, doncs, Gauss diferencia el seu llibre dels tractats d'aritmètica que, en un sentit tradicional, comprenien els coneixements de càlcul necessaris per a l'activitat mercantil.

La primera edició de l'obra aparegué l'any 1801, quan Gauss comptava 24 anys. Es féu en llatí, sota el títol *Disquisitiones Arithmeticæ*. És un llibre dens que conté prop de 700 pàgines plenes de fórmules. El seu format és l'usual avui: teoremes, demostracions, corol·laris, etc.; tot això il·lustrat amb nombrosos exemples.

L'obra fou editada a Leipzig, ciutat situada a la Saxònia. A l'època de Gauss, Leipzig era un centre intel·lectual i musical que ja comptava amb una llarga tradició en l'edició de llibres; la Universitat de Leipzig havia estat fundada l'any 1409 i la ciutat posseïa una població estudiantil important. Però, tot i l'experiència dels editors de Leipzig, el procés

Em plau agrair a la Facultat de Matemàtiques i Estadística de la Universitat Politècnica de Catalunya la invitació a participar en la Jornada Gauss, celebrada amb motiu de la commemoració dels 150 anys de la mort d'aquest insigne matemàtic, i per haver-me facilitat una transcripció de la conferència impartida, que ha estat la base d'aquest text.

Amb el suport parcial de MCYT, MTM2006-04895.

d'edició fou complex. Segons ens diu Gauss, el temps d'edició s'allargà durant quatre anys.

Les *Disquisitiones* han estat traduïdes al francès, l'any 1807; a l'alemany, l'any 1889; al rus, l'any 1959; a l'anglès, l'any 1965; al castellà, l'any 1995; i al català, l'any 1996. La traducció castellana fou publicada per l'Acadèmia Colombiana de Ciències Exactes, Físiques i Naturals. La traducció catalana és deguda a Griselda Pascual i Xufré i fou publicada per la Societat Catalana de Matemàtiques.[1]

En la primera part d'aquest escrit, parlaré de les circumstàncies que envoltaren la creació d'aquesta obra singular. En la segona part, faré una presentació sinòptica del seu contingut, acompanyada d'algunes reflexions sobre la seva significació en termes actuals. Per a les cites textuals i per als nombres de pàgines, empraré la traducció catalana.

1. Context històric

A la fi del segle XVIII, l'actual Alemanya estava constituïda per petits estats, els uns catòlics i els altres protestants, que estaven regits per governs absoluts. En els estats catòlics, l'ensenyament estava en mans de l'església; en els estats protestants, l'ensenyament era públic. La vida de Gauss transcorregué entre dues ciutats pertanyents a dos estats protestants: Brunsvic, que era la capital del ducat de Brunsvic-Lüneburg, i Gotinga, a l'estat de Hannover.

Gauss s'educà en el si d'una família humil. El seu pare s'ocupava en tota mena d'oficis. La seva mare havia treballat de soltera al servei d'una família benestant.

L'educació de Gauss fou finançada per un protector: Carles Guillem Ferran (1735-1806), duc de Brunsvic-Lüneburg, i príncep de Brunsvic-Lüneburg-Bevern des de l'any 1780. Es tractava d'un mariscal prussià que s'havia distingit a la Guerra dels Set Anys (1756-1763). Era nebot de Frederic II, El Gran, (1712-1786), rei de Prússia des de l'any 1740. Les corts germàniques no tenien la pompa de les corts franceses de

[1]Griselda Pascual treballà molts anys en la traducció de les *Disquisicions aritmètiques*. Per a la revisió de la traducció, comptà amb un equip assessor format per M. Otero-Vidal, llatinista; M. T. Sucarrats, filòloga catalana; A. Travesa i A. Violant, ambdós matemàtics.

FIGURA 1. Els estats on visqué Gauss

la mateixa època; en canvi, s'esmerçaven a protegir filòsofs, músics i científics. El príncep intentava traslladar a la seva cort l'ambient culte que havia aconseguit el seu oncle.

La família dels Brunsvic es remunta a l'any 1235 i formà diverses branques a Europa. Una d'elles és la dels electors de Hannover, d'on procedeix la família reial anglesa actual. Aquesta família està vinculada amb Barcelona a través de la figura d'Elisabet-Cristina de Brunsvic-Wolfenbüttel (1691-1750). Elisabet-Cristina es casà a Barcelona amb l'arxiduc Carles, el qual després esdevindria l'emperador Carles VI, en la numeració dels Àustries. Fou així emperadriu d'Àustria i reina de Catalunya i Aragó a partir del 1708. Fou la mare de Maria Teresa d'Àustria (1717-1780) i l'àvia, per tant, de Maria Antonieta (1755-1793).

Elisabet-Cristina i Carles són els Àustries que es retiren de Barcelona, l'any 1714, quan Catalunya passa a mans dels Borbó. No solament l'expulsió dels àrabs i dels jueus fou una ocasió perjudicial per al desenvolupament de la ciència en el nostre país, sinó també aquest altre

moment, en el qual persones interessades en les arts i les ciències abandonen Catalunya. (L'any 1717, Felip V clausurà les vuit universitats catalanes existents aleshores, concentrant els estudis universitaris en la Reial i Pontifícia Universitat de Cervera. La Universitat de Barcelona romangué tancada 120 anys, fins a la seva restauració, l'any 1837.)

A l'època de Gauss, l'ambient intel·lectual respirava una barreja de racionalisme i romanticisme. D'una banda, es tenia la mirada posada en els cànons clàssics; de l'altra, es parlava de l'alliberament de l'esperit i del seu retorn a la natura.

És el temps del moviment literari *Sturm und Drang* (1765-1785), que preconitzava la glorificació del geni (*Geniezeit*). Segons aquest corrent de pensament, les persones extraordinàriament dotades només han d'obeir els impulsos que els permeten la seva realització plena.

La Revolució Francesa, en el 1789, i les guerres napoleòniques, que s'estengueren entre els anys 1799 i 1815, són esdeveniments que repercutiren en la vida de Gauss.

Entre els coetanis de Gauss, destaquem: J. W. Goethe (1749-1832) i F. von Schiller (1759-1805), en literatura; I. Kant (1724-1804) i G. W. F. Hegel (1770-1831), en filosofia; W. A. Mozart (1756-1791) i L. van Beethoven (1770-1827), en música.

Pel que fa a les matemàtiques, L. Euler (1707-1783) morí quan Gauss comptava 6 anys. A. M. Legendre (1752-1833) i E. Galois (1811-1832) són contemporanis seus, a França; C. G. J. Jacobi (1804-1851) i P. G. L. Dirichlet (1805-1859) ho són a Alemanya; i N. H. Abel (1802-1829) ho és a Noruega.

Anys d'aprenentatge del jove Gauss

Atès que Gauss escriví les *Disquisicions* quan encara era estudiant, farem un repàs a la formació que va rebre. Si bé en cap moment no s'ha d'interpretar que l'obra fos producte d'aquella formació, val la pena remarcar que l'educació de Gauss fou prou liberal per no ofegar-ne el desenvolupament.

Gauss assistí a l'escola elemental als 7 anys. Allí tingué de mestre J. G. Büttner, qui, en captar el talent d'aquell nen per a les matemàtiques, encarregà a Hamburg la compra d'un *Tractat d'aritmètica* per tal que el pogués estudiar pel seu compte.

Als 11 anys, Gauss inicià els estudis a l'escola secundària o *Gymnasium*, institució en la qual es formà en matemàtiques, llatí i alemany culte. L'aprenentatge del llatí era un requisit indispensable per a poder seguir més endavant una carrera acadèmica.

Als 14 anys, Gauss fou presentat al príncep Carles Guillem Ferran i en rebé una beca de 10 tàlers l'any. Aquest tipus d'ajuts eren freqüents en aquells temps i són un precedent de les beques de l'actualitat.

Als 15 anys, Gauss ingressà en el *Collegium Carolinum*, una institució acadèmica estatal, moderna, orientada cap als estudis científics. El centre comptava amb una biblioteca excel·lent, on Gauss pogué familiaritzar-se amb obres de Newton, d'Euler i de Lagrange. Gauss inicià una amistat amb J. H. Meyerhoff, important en relació amb el llibre que ens ocupa. Meyerhoff, que estudià llengües clàssiques, ajudaria Gauss en la correcció i la millora del llatí de les *Disquisicions*.

Als 18 anys, Gauss es traslladà a la Universitat de Gotinga. Per a Gauss, anar a estudiar a Gotinga implicava anar-se'n a l'estranger, car aquesta ciutat pertanyia a l'estat de Hannover, diferent doncs de Lüneburg. El príncep hauria preferit que Gauss estudiés a la Universitat de Helmsted, fundada l'any 1569 i situada en el seu propi estat, però Gauss no ho va voler adduint l'excel·lència de la Biblioteca de la Universitat de Gotinga.

La Universitat de Gotinga havia estat fundada l'any 1737 pel rei Jordi II (1683-1760) d'Anglaterra, que era també príncep de Hannover. Seguia el model de les universitats angleses d'Oxford i de Cambridge, i tenia fama per la seva independència respecte de l'església i del govern.

En el decurs dels seus anys d'estudiant a la Universitat de Gotinga, tingué lloc l'eclosió del talent matemàtic de Gauss. Valdrà la pena que donem un cop d'ull al pla d'estudis que ho féu possible: a la Universitat de Gotinga, Gauss gaudí de llibertat acadèmica; és a dir, no va tenir cap tutor; tampoc no hagué de sotmetre's ni a cap examen ni a cap tipus de control curricular. A Gotinga, Gauss estudià astronomia i

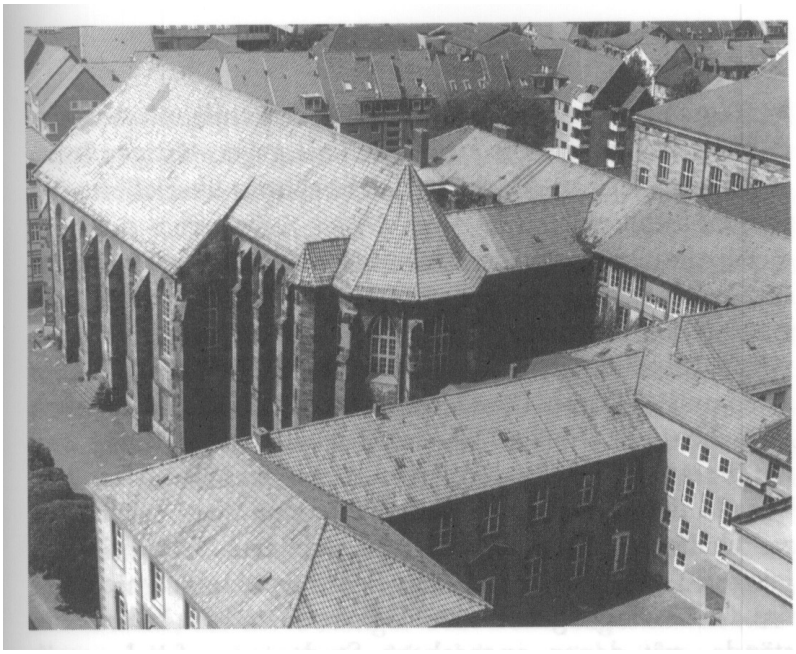

FIGURA 2. Església de Sant Pau de Gotinga

FIGURA 3. Museu d'Arts i de Ciències de Hannover

FIGURA 4. Auditori de la Universitat de Gotinga (1865)

física. Pel que sembla, amb A. G. Kästner (1719-1800), professor de matemàtiques d'aquella institució, no s'entengueren del tot.

Quan comptava 19 anys, aquell jove estudiant descobrí que el polígon regular de 17 costats és construïble amb regle i compàs i, segons ell mateix explica, s'adonà dels principis generals que permeten la caracterització dels polígons regulars construïbles amb aquests instruments. Exposà els seus resultats a Kästner, que no se'n féu ressò. Però el goig d'aquella descoberta decantà Gauss definitivament pels estudis de ciències, per davant dels de llengües clàssiques.

A la seva època d'estudiant a Gotinga, Gauss féu amistat amb W. Bolyai (1775-1856), un noble de Transilvània, aleshores estudiant de filosofia. En aquells anys, els estudis de filosofia comprenien una part dedicada a les matemàtiques. En el paràgraf següent, Bolyai explica quina era la seva relació amb Gauss i com era Gauss d'estudiant:

> Vaig conèixer Gauss, que aleshores era un estudiant a Gotinga, i amb qui encara mantinc un contacte amical, malgrat que mai no podré comparar-me amb ell. Era molt modest i no es feia valer gaire. No solament durant tres dies, com Plató, sinó també durant anys, hauria

> pogut estar al seu costat i no adonar-me de la seva grandesa. Dissortadament, no vaig saber obrir aquell llibre innominat, silent, i llegir-lo. Ignorava que sabés tantes coses. Ell, en veure com era jo, em tenia una gran consideració, passant per alt les meves limitacions. Compartíem la passió (invisible) per les matemàtiques i per les nostres conviccions morals; sovint caminàvem plegats, cadascú lliurat als seus propis pensaments, sense intercanviar cap paraula, durant hores.

Amb els anys, W. Bolyai esdevingué professor de matemàtiques, física i química a la ciutat de Marosvásárhely. S'interessà pels fonaments de la geometria, la filosofia, la música i les arts dramàtiques. Fou el pare de J. Bolyai (1802-1860), un dels primers matemàtics que es dedicà a l'estudi de les geometries no euclidianes.

La il·lustració 2 correspon a l'Església de Sant Pau de Gotinga, en la qual estava ubicada la biblioteca de la universitat quan Gauss hi estudiava. Avui, l'edifici és seu d'una biblioteca i és una sala d'exposicions.

La il·lustració 4 correspon a una vista actual de l'Auditori de la Universitat de Gotinga. L'edifici fou construït l'any 1865 i és obra de l'arquitecte Friedrich Doeltz. Té com a precedent l'edifici del Museu d'Arts i Ciències de Hannover (il·lustració 3). És remarcable l'analogia d'aquestes dues construccions amb l'edifici històric de la Universitat de Barcelona, obra d'Elias Rogent (1821-1897) construïda entre els anys 1863 i 1889.

En finalitzar els seus estudis a Gotinga, Gauss presentà les *Disquisicions* al príncep Carles Guillem Ferran. Aquest, però, considerà que les *Disquisicions* no eren suficients per a justificar la beca que li havia proporcionat durant tots aquells anys. Aquesta pot semblar una decisió una mica estranya, però, de totes maneres, ignorem quina era la longitud del text en aquell moment. Recordem que Gauss ens ha dit que l'obra fou completada en el decurs del llarg període de la seva impressió. Gauss hagué de presentar una tesi doctoral a la Universitat de Helmsted, a l'estat del Príncep.

El tema de la tesi de Gauss fou la demostració del teorema fonamental de l'àlgebra. El seu director fou J. F. Pfaff (1765-1825), professor a Helmstedt i deixeble de Kästner. Gauss presentà la tesi l'any 1799. El grau de doctor li fou concedit *in absentia*, i se'l lliurà de l'examen oral habitual, o defensa de la tesi.

Pfaff dirigí únicament dos alumnes al llarg de la seva vida: Gauss i A. F. Möbius però, això no obstant, compta avui amb 39115 (37707 + 1408) descendents.

L'any 1804, Gauss retornà a Brunsvic. Poc després, comentà satisfet en una carta a Wilhelm Olbers que un jove de París estava estudiant les *Disquisicions*:

> Fa poc he tingut el gust de rebre una carta de LeBlanc, un jove geòmetre de París molt familiaritzat amb la matemàtica d'alt nivell, que m'ha fet palès el profund coneixement que té de les meves *Disquisicions Aritmètiques*.

El 14 d'octubre de 1806 tingueren lloc les batalles de Jena i d'Auerstädt contra les tropes napoleòniques. En aquesta última, el príncep protector de Gauss, que comandava les tropes, fou ferit de mort.

Gauss s'assabentà que ell, en el decurs dels enfrontaments amb Napoleó, havia estat protegit per la intercessió d'una dama francesa: Sophie Germain (1776-1831). Germain no era altra que *el jove* M. LeBlanc. La correspondència entre Gauss i Germain s'estengué entre els anys 1806 i 1809, sense que s'arribessin a conèixer personalment. Gauss proposà que Germain rebés un doctorat *honoris causa* per la Universitat de Gotinga, però ella morí abans que la universitat s'hagués pronunciat sobre aquest afer.

L'any 1807, Gauss retornà a Gotinga, però ara desproveït de la protecció del príncep.

Després de la primera edició de les *Disquisicions Aritmètiques*, l'editor que suposadament havia de distribuir l'obra es declarà en fallida. Moltes còpies es perderen. Com a resultat, els deixebles de Gauss havien de copiar a mà els seus passatges. A Alemanya, la situació començà a canviar només a partir del 1840, quan Dirichlet n'emprengué l'estudi i començà a impartir classes sobre el text. A partir d'aleshores, la influència del seu contingut ja no s'aturaria.

2. Disquisicions Aritmètiques

En el pròleg de l'obra, Gauss agraeix la liberalitat del *Príncep sereníssim*, el seu benefactor, amb aquestes paraules:

> Penso que ningú no ignora que és habitual en *Tu* una tan insigne liberalitat vers tots els que sembla que es dediquen a cultivar les millors disciplines, i que no són excloses del *Teu* patrocini aquelles ciències que són considerades per la gent més abstruses i més allunyades de la utilitat de la vida comuna, perquè *Tu* mateix t'adones fins a l'arrel de l'íntim i necessari vincle de totes les ciències entre elles, amb una ment molt sàvia i molt coneixedora de totes les coses que interessen per tal d'augmentar la prosperitat de la societat humana.

En el fragment següent del prefaci de les *Disquisicions*, Gauss dóna la seva visió de l'aritmètica superior:

> Pertany a l'Aritmètica Superior allò que Euclides va transmetre en els Elements, L. VII i s., amb l'elegància i el rigor habituals en les obres dels antics; no obstant això es limita als primers inicis d'aquesta ciència. La cèlebre obra de Diofant [...] conté moltes qüestions que susciten una no gens mediocre estimació pel que fa a l'enginy i agudesa de l'autor [...]. Sembla que aquest llibre fa època en la història de les Matemàtiques, més perquè posa els primers fonaments d'un art característic i de l'Àlgebra, que perquè faci progressar l'Aritmètica Superior amb nous descobriments. [...] Molt més es deu als moderns [...] com P. de Fermat, L. Euler, L. La Grange, A. M. Le Gendre [...]. Aquí m'abstinc d'enumerar, però, quines coses descobertes per cadascun d'aquests geòmetres són útils [...]; la majoria seran lloades en el seu lloc d'aquestes *Disquisicions Aritmètiques*.

Quan Gauss inicià la redacció de les *Disquisicions Aritmètiques*, era coneixedor de bona part de les contribucions aritmètiques degudes a Fermat, Euler, Lagrange i Legendre. Si algun d'aquests autors havia tractat prèviament un dels temes que ell considera, té cura de fer-ho constar. Amb tot, però, hi va haver conflictes.

L'any 1798, quan l'obra de Gauss era ja a l'impremta (però tres anys abans de sortir publicada) aparegué l'edició de l'obra de Legendre *Essai d'une théorie des nombres*. No sabem exactament fins a quin punt l'assaig de Legendre influí en la redacció final de les *Disquisicions*. Si bé la presentació i el contingut de les dues obres és diferent, ambdues tenen, certament, punts importants en comú. Gauss ens ho explica en les paraules següents:

> S'ha de tenir present que jo, quan al començament del 1795 vaig dedicar la meva ment a aquest tipus de disquisicions, desconeixia totes les que havien estat elaborades pels més moderns en aquest camp i estava privat de tots els recursos mitjançant els quals hauria pogut assabentar-me una mica d'aquestes qüestions. Sens dubte, ocupat aleshores per casualitat en una altra feina, vaig anar a parar a una extraordinària veritat aritmètica (fou, efectivament, si no m'equivoco, el teorema de l'article 108).
>
> Mentrestant, va sortir l'obra egrègia d'un home, anteriorment digne de gran mèrit en el camp de l'Aritmètica Superior, *Le Gendre*, *Essai d'une théorie des nombres* en què no només va recollir escrupolosament i va resumir per ordre el que s'havia elaborat fins aleshores en aquesta ciència, sinó que també va afegir-hi, a més a més, moltes coses de la seva pròpia collita. Com que aquest llibre seriós em va arribar a les mans després que la major part de l'obra ja estigués transcrita a la impremta, no fou possible mencionar-lo en cap lloc on l'analogia dels plantejaments podia donar-hi peu; només, respecte a uns quants punts, semblava necessari incorporar als Apèndixs algunes observacions que l'autor, molt culte i molt brillant, interpretarà, confio, benèvolament.

El punt comú més important entre els dos textos de Legendre i de Gauss és la llei de reciprocitat quadràtica, l'extraordinària veritat matemàtica a la qual Gauss ha fet referència. Per les paraules de Gauss, aquest hi arribaria abans de la lectura de Legendre. Però el fet que Gauss s'atribuís la descoberta de la llei de reciprocitat disgustà Legendre. Gauss, però, fou el primer a donar-ne una demostració completa. L'any 1808, Legendre publicà una segona edició de l'*Essai d'une théorie des nombres* en la qual introduí alguns resultats de les *Disquisicions*.

En la història de les matemàtiques es repeteix sovint que persones de països i cultures diferents arriben simultàniament als mateixos resultats. Aquest fet, que és font permanent de conflictes i de disgustos, sembla inevitable. En el cas de la llei de reciprocitat quadràtica, el mèrit de la seva descoberta caldria repartir-lo entre Euler, Legendre i Gauss.

Contingut

El contingut de les *Disquisitions aritmètiques* està dividit en set seccions (o capítols) diferents:

Secció primera: De les congruències numèriques en general

Secció segona: De les congruències de primer grau

Secció tercera: Dels residus de potències

Secció quarta: De les congruències de segon grau

Secció cinquena: De les formes i equacions indeterminades de segon grau

Secció sisena: Aplicacions diverses de les disquisicions precedents

Secció setena: De les equacions que defineixen les seccions del cercle

Per a llegir les *Disquisicions* no calen coneixements previs. És una obra de joventut, autocontinguda, que pot ser llegida pel jovent. Però per a assimilar-ne el contingut calen, a banda de llapis i paper, moltes hores d'estudi.

Gauss deriva d'una manera natural i coherent propietats dels nombres, que demostra rigorosament. Gauss il·lustra qualsevol definició o raonament, per senzills que siguin, mitjançant exemples numèrics (un costum que avui es practica molt poques vegades i que, de mantenir-se, representaria per als lectors un estalvi considerable de temps). A continuació, comentarem alguns resultats de cada secció.

Secció primera. De les congruències numèriques en general

La secció té 7 pàgines. Gauss comença per exposar un recull de resultats sobre congruències, la majoria dels quals eren ben coneguts per Euler.

Per a designar que dos nombres són congrus, introdueix el símbol que ha esdevingut habitual: la notació

$$a \equiv b \pmod{m}$$

equival a dir que el nombre m, que anomena mòdul, divideix la diferència $a - b$. Considera els exemples

$$-16 \equiv 9 \pmod{5}, \quad -7 \equiv 15 \pmod{11}$$

i ens diu que

> hem adoptat aquest signe per la gran analogia que es troba entre la igualtat i la congruència.

Després de fer un estudi general de les congruències i de les seves propietats més bàsiques, demostra els criteris clàssics de divisibilitat:

$$a + 10b + 100c + \cdots \equiv a + b + c + \ldots \pmod 3,$$
$$a + 10b + 100c + \cdots \equiv a + b + c + \ldots \pmod 9,$$
$$a + 10b + 100c + \cdots \equiv a - b + c - \cdots \pmod{11}.$$

Tot seguit explica la prova del 9, basada en el criteri de divisibilitat per 9 i en el fet que si $a = bq + r$, aleshores $a \equiv bq + r \pmod 9$.

Secció segona. De les congruències de primer grau

La secció té 35 pàgines. Gauss hi estudia les congruències de primer grau

$$ax + b \equiv c \pmod p,$$

on p és un nombre primer, així com també els sistemes lineals de congruència i les equacions polinòmiques de congruència en una indeterminada de grau superior.

Gauss demostra la propietat següent:

> Si ni a ni b es poden dividir per un nombre primer p, el producte ab tampoc no es podrà dividir per p.

La propietat anterior intervé en la prova de la unicitat de la descomposició dels nombres enters en factors primers. Avui és coneguda amb el nom de condició de Gauss. La propietat en qüestió, però, es troba ja en Euclides, *Elements*, VII, 24, tal com ho observa Gauss:

> Una demostració d'aquest teorema ja fou transmesa per Euclides.

De totes maneres, Euclides no esmenta la unicitat de la factorització d'un enter en producte de primers. La unicitat és un teorema de les *Disquisicions*:

> Un nombre compost qualsevol només es pot descompondre en factors primers d'una sola manera.

Tot seguit Gauss estudia el màxim comú divisor i el mínim comú múltiple de dos nombres, l'algoritme d'Euclides, proporciona un algoritme per a resoldre les congruències de primer grau i exposa el que avui s'anomena teorema xinès dels residus:

> De la recerca d'un nombre congru a residus donats segons mòduls donats.

En aquesta mateixa secció desenvolupa la teoria general per a la resolució de sistemes de congruències lineals. Per exemple, el sistema

$$\begin{cases} 3x + 5y + z & \equiv 4 \\ 2x + 3y + 2z & \equiv 7 \\ 5x + y + 3z & \equiv 6 \end{cases} \pmod{12}$$

admet per solucions

$$\{(2, 11, 3), (5, 11, 6), (8, 11, 9), (11, 11, 0)\}.$$

Observem que el sistema anterior és un sistema d'equacions lineals de coeficients en l'anell de classes de residus $\mathbb{Z}/12\mathbb{Z}$, que té divisors de zero. El discriminat del sistema no és primer amb el mòdul, per la qual cosa la matriu no és invertible, però Gauss en dóna la solució completa.

En exemples com l'anterior, s'aprecien les tècniques de Gauss per a la resolució de sistemes lineals. Entre d'altres, les *Disquisicions* són un precedent de l'àlgebra lineal. Cal tenir present que a l'època l'àlgebra lineal no estava desenvolupada, ni tampoc ho estava el càlcul matricial. Quan Gauss necessita compondre matrius, per exemple, realitza les substitucions *a mà*.

En aquesta secció, Gauss recupera també resultats d'Euler relatius al seu indicador, la funció $\varphi(A)$:

> Trobar quants nombres positius hi ha no més grans que un nombre positiu donat A i simultàniament primers amb ell. [...] La primera solució d'aquest problema apareix en els comentaris de l'il·lm. Euler.

A les *Disquisicions*, Gauss atorga gairebé sempre el tractament d'il·lustríssims a Euler i a Lagrange; i de preclar a Legendre. No així a Fermat, a qui sol qualificar de sagaç.

El resultat següent fa referència al nombre d'arrels que pot tenir un polinomi de grau m en un cos de p elements.

> La congruència de m-èsim grau
>
> $$Ax^m + Bx^{m-1} + Cx^{m-2} + \cdots + Mx + n \equiv 0,$$
>
> el mòdul de la qual és un nombre primer p que no divideix A, no pot ser resolta de més de m maneres diferents; o sigui, no té més de m arrels incòngrues segons p.
>
> Aquest teorema va ser proposat i demostrat per primera vegada per l'il·lm. La Grange. Apareix també en la dissertació de l'il·lm. Le Gendre. L'il·lm. Euler demostrà que la congruència $x^n - 1 \equiv 0$, el mòdul de la qual és un nombre primer p, no pot tenir més de n arrels diferents.

És difícil precisar si aquest teorema fou conegut per Gauss abans de la seva demostració del teorema fonamental de l'àlgebra. Quan Gauss lliurà les *Disquisicions* a la impremta, encara no havia llegit la tesi, però no sabem si el teorema anterior fou afegit durant el període d'edició de l'obra.

Secció tercera. Dels residus de potències

La secció té 50 pàgines. Gauss hi demostra el petit teorema de Fermat, el teorema de Wilson i l'existència d'arrels primitives. La secció conté, també, uns apartats sobre el càlcul amb índexs.

Donat un nombre primer p, Gauss demostra que la congruència

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

és satisfeta per tots els nombres enters a tals que $p \nmid a$. Atribueix la descoberta d'aquest resultat a Fermat:

> Aquest teorema, que, tant per causa de la seva elegància com per causa de la seva extraordinària utilitat, és digne de tota l'atenció, se sol anomenar *teorema de Fermat*, pel seu descobridor.

Dóna dues demostracions del petit teorema de Fermat, la segona de les quals empra la fórmula del binomi:

$$(a + b + c + \cdots)^p \equiv a^p + b^p + c^p + \cdots \pmod{p}.$$

Si bé Gauss no féu explícita la definició de grup, aquest concepte és implícit en molts passatges de les *Disquisicions*. Per exemple, en l'estudi que realitza de les arrels primitives. En termes actuals, una arrel primitiva mòdul un nombre primer p és un generador del grup multiplicatiu de les classes de residus mòdul p. En considerar les arrels primitives segons un mòdul, Gauss posa de manifest el seu coneixement dels resultats d'Euler.

> Anomenarem *arrels primitives*, com l'il·lm. Euler, els nombres que pertanyen a l'exponent p. Elegirem com plagui una arrel primitiva a com a *base*.

Tot seguit, Gauss caracteritza els mòduls per als quals existeixen arrels primitives. Aquests són

$$2,\ 4,\ p^n,\ 2p^n, \quad \text{on } n \geq 1,\ \ p \text{ primer.}$$

Observa que el càlcul amb arrels primitives és semblant al càlcul amb logaritmes. Si a és una arrel primitiva mòdul p, i $a^e \equiv b \pmod{p}$, Gauss escriurà

$$\operatorname{Ind} b = e.$$

> Els teoremes que pertanyen als índexs són completament anàlegs als dels logaritmes.

En prendre $p = 19$ i $a = 2$, proporciona l'exemple següent de taula d'índexs.

$p = 19, \quad a = 2$

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

A partir de l'estudi previ de les equacions lineals de congruència i de la taula anterior, obté totes les arrels quinzenes de 11 mòdul 19:

$\sqrt[15]{11} \pmod{19}; \quad x^{15} \equiv 11 \pmod{19}.$

$15 \operatorname{Ind} x \equiv \operatorname{Ind} 11 \equiv 12 \pmod{18}; \quad \operatorname{Ind} x \in \{2, 8, 14\}, \quad x \in \{4, 9, 6\}.$

Veiem, doncs, que el contingut de les tres primeres seccions és bàsicament una recopilació de resultats coneguts però dispersos en treballs d'autors diferents.

Secció quarta. De les congruències de segon grau

La secció quarta té 69 pàgines. Es tracta d'estudiar les equacions de congruència de segon grau

$$ax^2 + bx + c \equiv 0 \pmod{p},$$

en les quals a, b, c, p són nombres enters i p és primer. Per a tal fi, Gauss estudia primerament l'existència d'arrels quadrades mòdul un nombre primer p. Si un enter a és un quadrat mòdul p, escriu $a\mathrm{R}p$; altrament, $a\mathrm{N}p$.

Per a distingir els residus quadràtics cal dir que és més còmode la notació de Legendre, que és la que avui s'utilitza en els textos:

$$\begin{cases} \left(\dfrac{a}{p}\right) = 1 & \text{si } p \nmid a,\ a\mathrm{R}p; \\ \left(\dfrac{a}{p}\right) = -1 & \text{si } p \nmid a,\ a\mathrm{N}p; \\ \left(\dfrac{a}{p}\right) = 0 & \text{si } p \mid a. \end{cases}$$

Els càlculs condueixen Gauss a comparar, donats dos primers senars diferents p i q, l'existència d'arrels quadrades de q mòdul p amb l'existència d'arrels quadrades de p mòdul q; és a dir, a l'estudi simultani de les equacions

$$x^2 \equiv q \pmod{p}; \quad y^2 \equiv p \pmod{q}.$$

S'adona que l'existència d'arrels en un cas està condicionada per l'existència o no d'arrels en l'altre. L'enunciat precís d'aquest fet constitueix la llei de reciprocitat quadràtica. Gauss designa aquesta llei amb el nom de teorema fonamental i considera que és el resultat més rellevant de l'obra.

Escrita la llei de reciprocitat en funció del símbol de Legendre, el seu enunciat és el següent:

Donats p, q, primers senars, se satisfà que

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

Al llarg de la seva vida, Gauss donà 6 demostracions diferents de la llei de reciprocitat. Recordem, però, que ni el nom de llei de reciprocitat ni el símbol de Legendre figuren en les *Disquisicions.*

La primera demostració de la llei donada a les *Disquisicions* és per inducció:

> Direm que el teorema fonamental és veritat fins a algun nombre M, si val per a dos nombres primers qualssevol cap dels quals no supera M.

Per a portar a terme la inducció, distingeix casos diferents. La metodologia emprada en la demostració és la següent: primerament estudia molts exemples particulars dins d'una mateixa situació, després dedueix quin ha de ser el comportament general en aquell cas i finalment demostra per inducció el resultat que ha intuït, segons ens diu, per indici.

Per començar a veure quin és el funcionament general, parteix de la taula següent:

	-1	2	3	5	7	11	$\cdots$	97
3			$-$		$-$		$\cdots$	$-$
5	$-$			$-$		$-$	$\cdots$	
7		$-$			$-$	$-$	$\cdots$	
11			$-$	$-$		$-$	$\cdots$	$-$
13	$-$		$-$				$\cdots$	
17	$-$	$-$					$\cdots$	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
97	$-$	$-$	$-$			$-$	$\cdots$	$-$

A la taula, el signe $-$ indica que l'entrada de la columna que el conté és un residu quadràtic mòdul l'entrada de la fila corresponent. Altrament,

no escriu cap signe. Aleshores passa a veure per a quins parells hi ha simetria i per a quins no n'hi ha. Així, ens diu:

> -1 és residu dels nombres 5, 13, 17, 29, 37, originat pels quadrats dels nombres 2, 5, 4, 12, 6.
> -1 no és residu dels nombres 3, 7, 11, 19, 23.

Vist això, dedueix un teorema per indici:

> quan els nombres primers són congrus amb 1 mòdul 4, -1 és residu i, quan són congrus amb 3 mòdul 4, aleshores -1 no és residu.

Copsat l'indici, procedirà a la demostració del teorema. Vegem els diferents casos que considera i alguns dels seus comentaris.

- El residu -1

> -1 és residu quadràtic de tots els nombres primers de la forma $4n+1$, però no-residu de tots els nombres primers de la forma $4n+3$.
>
> Aquesta demostració també es deu a l'il·lm. Euler.

- Els residus ± 2:

> $+2$ és no-residu de tots els nombres primers de la forma $8n+3$; però -2, residu.
> Tant -2 com $+2$ són no-residus de tots els nombres primers de la forma $8n+5$.
> -2 és no-residu de tots els nombres primers de la forma $8n+7$; però $+2$, residu.
> Tant -2 com $+2$ són residus de tots els nombres primers de la forma $8n+1$.

En aquest cas comenta:

> Aquests teoremes elegants ja foren coneguts pel sagaç Fermat. Però no va comunicar mai la demostració que va declarar que tenia. Posteriorment va ser investigada, sempre en va, per l'il·lm. Euler; l'il·lm. La Grange va trobar el primer una demostració rigorosa.

- Els residus ± 3, ± 5, ± 7, ... En el cas ± 3, diu:

> Les proposicions que pertanyen als residus $+3$ i -3 ja foren conegudes per Fermat. Però l'il·lm. Euler va transmetre el primer les demostracions. Per això és més sorprenent que les demostracions que pertanyen

> als residus $+2$, -2, basades en artificis completament similars, sempre haguessin fugit de la seva sagacitat.

Analitzats aquests casos, estableix per indici el teorema general:

> Si p és un nombre primer de la forma $4n+1$, $+p$ serà residu o bé no-residu de qualsevol nombre primer que, pres positivament, és residu o bé no-residu de p; però si p és de la forma $4n+3$, ho serà $-p$.

La demostració rigorosa del cas general, o de la llei de reciprocitat pròpiament dita, ocupa 30 pàgines. Gauss cita Legendre com segueix:

> El preclar Le Gendre també va intentar la demostració, de la qual, com que és extremament enginyosa, en parlarem més extensament a la secció següent. Però com que en ella va suposar molt sense demostració [...], la nostra demostració s'haurà de tenir per la primera.

En una pretesa demostració de la llei de reciprocitat, Legendre havia utilitzat el fet que tota progressió aritmètica, en la qual el primer terme i la diferència són enters relativament primers, conté infinits nombres primers. A Gauss, amb raó, aquesta suposició no li semblà evident. L'afirmació de Legendre esdevingué anys després el teorema de la progressió aritmètica, provat per Dirichlet. El teorema de Dirichlet demostra, al mateix temps, que els primers es distribueixen equitativament en les classes de residus relativament primeres amb el mòdul. La demostració que donà Dirichlet no ha estat millorada; es basa en l'estudi de sèries L associades a caràcters de grups finits i en propietats de funcions analítiques que Gauss encara no tenia a l'abast.

Després de demostrar el teorema fonamental, Gauss determina, per mitjà de factoritzacions, donats dos enters P, Q quan Q és un residu mòdul P. La secció conclou amb la reducció de l'estudi de les congruències $ax^2+bx+c \equiv 0 \pmod{p}$ a l'estudi de les congruències, dites pures,

$$x^2 \equiv Q \pmod{P}.$$

En l'actualitat, la llei de reciprocitat quadràtica s'explica en els cursos de teoria de nombres en una hora de classe. Una de les proves més habitual empra cossos finits i propietats elementals de sumes de Gauss.

Lleis de reciprocitat

La llei de reciprocitat quadràtica és la primera d'un conjunt de lleis aritmètiques, dites també de reciprocitat, que serveixen per a entendre el comportament dels nombres enters a partir dels nombres enters algebraics que en resulten per extensions finites. En tots els casos, les lleis de reciprocitat tenen cura del comportament dels ideals primers en extensions finites de cossos de nombres. Aquestes lleis són importants en la mesura que repercuteixen en l'estudi de les equacions diofantines.

La recerca de lleis de reciprocitat fou empresa per moltes altres persones. Gauss mateix intentà generalitzar la llei de reciprocitat del cas quadràtic a residus de potències més altes.

En l'estudi de les lleis de reciprocitat, podem distingir etapes diferents. La primera etapa s'inicià amb Fermat i finalitzà amb les recerques de Gauss. Formulada en termes d'extensions i de divisibilitat d'ideals, la llei de reciprocitat quadràtica té cura de les descomposicions dels ideals primers de $\mathbb{Z}$ en els anells dels enters dels cossos quadràtics.

Una segona etapa s'inicià amb Kummer i Eisenstein, amb l'estudi de les lleis de reciprocitat lligades als cossos ciclotòmics i a cossos cúbics. Kummer n'emprengué l'estudi arran de les seves investigacions sobre el teorema de Fermat. En aquest context, són remarcables els treballs del propi Kummer, així com també els de Kronecker i de Weber, que caracteritzen les extensions abelianes del cos dels nombres racionals com a subcossos dels cossos ciclotòmics. A aquests resultats cal afegir els proporcionats per la teoria de la multiplicació complexa, que determina les extensions abelianes dels cossos quadràtics imaginaris i en proporciona les lleis de reciprocitat.

Una tercera etapa es desenvolupà arran de la teoria de cossos de classes. Tracta l'estudi de les extensions abelianes d'un cos de nombres qualsevol i de les lleis de reciprocitat que li són associades. La demostració dels resultats coneix presentacions diferents: cohomològica, analítica, local-global, etc.

La quarta etapa s'inicià amb l'estudi aritmètic d'algunes extensions no abelianes de cossos de nombres i de l'obtenció de les seves lleis de reciprocitat. La manera d'abordar aquest estudi és per mitjà del concepte de representació galoisiana. La dificultat augmenta amb la

dimensió de la representació. La teoria de cossos de classes es pot reformular en termes de representacions galoisianes de dimensió 1. Avui ja es compta amb resultats en dimensió 2. Hi ha treballs profunds per a les lleis de reciprocitat associades a representacions galoisianes de dimensió 2 de determinant senar. El marc general d'aquest estudi, en qualsevol dimensió, constitueix el programa de Langlands.

En la relació cronològica que segueix, figuren alguns autors que s'han ocupat d'aquestes qüestions.

P. Fermat,	1607-1665
L. Euler,	1707-1783
A. M. Legendre	1752-1833
C. F. Gauss	1777-1855
E. Kummer	1810-1893
F. Eisenstein	1823-1852
L. Kronecker	1823-1891
H. Weber	1842-1913
T. Takagi	1875-1960
E. Artin	1898-1962
H. Hasse	1898-1979
A. Weil	1906-1998
C. Chevalley	1909-1984
J. Tate	1925-
M. Eichler	1912-1992
J-P. Serre	1926-
G. Shimura	1928-
R. Langlands	1936-

Secció cinquena. De les formes i equacions indeterminades de segon grau

És la secció més extensa, car conté 363 pàgines. En aquesta secció, la força creativa de Gauss es manifesta en tota la seva potència. Si bé la secció també conté resultats en comú amb Fermat, Lagrange i Legendre, els resultats obtinguts per Gauss ultrapassen les recerques que els precediren.

L'objectiu de la secció és l'estudi de les formes quadràtiques binàries i dels enters que representen; és a dir, l'estudi de les equacions

$$ax^2 + 2bxy + cy^2 = d,$$

en les quals a, b, c, d són enters. El nombre $b^2 - ac = D$ és anomenat el determinant de la forma.

En relació amb aquest problema, Gauss coneixia els resultats d'Euler i de Fermat relatius a l'estudi de les sumes de dos quadrats ($a = c = 1, b = 0$), i alguns casos particulars més tractats per Legendre.

Gauss comença la secció classificant les formes quadràtiques binàries per mitjà de canvis lineals invertibles. En el llenguatge actual, es tracta de canvis de base definits per matrius del grup especial modular $\mathbf{SL}(2, \mathbb{Z})$, o bé del grup modular $\mathbf{GL}(2, \mathbb{Z})$. En el primer cas, Gauss parla d'equivalència pròpia. A continuació, Gauss dóna un criteri per a escollir el representant més senzill dins de cada classe de formes. D'aquesta manera obté les anomenades formes reduïdes.

El procés de reducció de formes és diferent segons que el determinant D sigui positiu o negatiu. En el cas $D < 0$, cada classe dóna lloc a un únic representant reduït. En el cas $D > 0$, no quadrat, hi pot haver formes reduïdes equivalents, que s'agrupen en cicles. Per completesa, Gauss també estudia els casos en què D és un quadrat no nul i el cas en què $D = 0$. En aquestes situacions, les formes descomponen en producte de formes lineals i Gauss remet la representació d'enters al seu estudi previ de les equacions diofantines lineals en dues incògnites. Per mitjà de la consideració de les formes reduïdes, Gauss demostra que el nombre de classes de formes d'un determinant donat és finit.

Tot seguit resol el problema de la representabilitat dels enters per formes d'un determinant donat. És a dir, donats un enter i un determinant, Gauss pot dir si l'enter serà representat o no per una de les classes de formes d'aquell determinant. En particular, recupera els teoremes clàssics sobre els enters que són expressables com a suma de dos quadrats; aquest és un cas que correspon a un nombre de classes igual a 1.

Gauss agrupa les classes de formes en ordres i en gèneres. [2] Els ordres consten de classes de formes del mateix discriminant i amb el mateix màxim comú divisor dels coeficients de la forma. Quan aquest màxim comú divisor és igual a 1, l'ordre s'anomena primitiu.

El concepte de gènere sorgeix en Gauss arran del fet següent. En tenir present que la classificació de les formes es fa per mitjà de matrius invertibles de coeficients enters, és evident que formes equivalents representen els mateixos nombres. Però Gauss s'adona que formes del mateix determinant que representin els mateixos nombres no tenen perquè ser equivalents. Aleshores les seves classes formaran part d'un mateix gènere.

Tot seguit considera una composició de formes, que fa extensiva a una composició de classes, d'ordres i de gèneres de formes. Arriba per composició de clases de formes de determinant donat a l'estructura algebraica d'un grup abelià finit. Especialment important és el grup abelià que sorgeix de les classes de formes pròpiament primitives.

Inicia en la mateixa secció un estudi de les formes quadràtiques ternàries, però només en aquells aspectes que li proporcionen informació addicional sobre les formes quadràtiques binàries.

En representar formes binàries per la ternària especial $x_1 - 2x_2\,x_3$, Gauss demostra l'existència de gèneres per a exactament la meitat dels caràcters totals associats a un discriminant. Aquests es calculen per mitjà de la llei de reciprocitat quadràtica aplicada a les expressions

$$\left(\frac{a}{p}\right), \quad p \mid D, \quad p \nmid a.$$

Els diferents gèneres es caracteritzen per la igualtat dels símbols anteriors, calculats sobre els nombres representats per la forma. Gauss demostra que tots els gèneres d'un mateix ordre contenen el mateix nombre de classes. Calcula el nombre de classes ambigües de determinant donat, que són els elements d'ordre dos del grup de classes.

[2] Aquesta classificació tan ben organitzada evoca la de Carl von Linné (1707-1778), naturalista suec de l'època que havia aplicat les categories aristotèliques a la classificació dels éssers vius. Segons Linné, aquests es divideixen en classes, ordres, gèneres i espècies.

Il·lustrarem alguns d'aquests resultats amb exemples de les *Disquisicions*.

• $D = -85$. Tenim vuit classes de formes quadràtiques binàries amb aquest discriminant. Els seus representants reduïts són:

$$(1,0,85), \qquad (2,1,43), \qquad (5,0,17), \qquad (10,5,11),$$

$$(-1,0,-85), \quad (-2,1,-43), \quad (-5,0,-17), \quad (-10,5,-11).$$

• $D = 79$. Les formes reduïdes indefinides d'aquest discriminant es distribueixen en sis períodes:

I. $(1,8,-15),(-15,7,2),(2,7,-15),(-15,8,1),$

II. $(-1,8,15),(15,7,-2),(-2,7,15),(15,8,-1),$

III. $(3,8,-5),(-5,7,6),(6,5,-9),(-9,4,7),(7,3,-10),(-10,7,3),$

IV. $(-3,8,5),(5,7,-6),(-6,5,9),(9,4,-7),(-7,3,10),(10,7,-3),$

V. $(5,8,-3),(-3,7,10),(10,3,-7),(-7,4,9),(9,5,-6),(-6,7,5),$

VI. $(-5,8,3),(3,7,-10),(-10,3,7),(7,4,-9),(-9,5,6),(6,7,-5).$

• $D = 79$. Totes les representacions del nombre 585 per la forma

$$42x^2 + 62xy + 21y^2$$

estan contingudes en les quatre fórmules paramètriques:

$$\begin{array}{ll} x = 6t - 123u, & y = -3t + 159u, \\ x = 66t - 597u, & y = -69t + 633u, \\ x = 3t - 114u, & y = t + 157u, \\ x = 83t - 746u, & y = -87t + 789u, \end{array}$$

on t, u, denoten formalment tots els nombres enters que satisfan l'equació

$$t^2 - 79u^2 = 1,$$

anomenada de Pell–Fermat. Les solucions d'aquesta equació s'expressen per les fórmules

$$\begin{aligned} \pm t &= \tfrac{1}{2}\left((80 + 9\sqrt{79})^e + (80 - 9\sqrt{79})^e\right), \\ \pm u &= \tfrac{1}{2}\sqrt{79}\left((80 + 9\sqrt{79})^e - (80 - 9\sqrt{79})^e\right), \quad e \geq 1. \end{aligned}$$

• $D = -161$. Les classes de formes definides es distribueixen en quatre gèneres, cadascun dels quals conté quatre classes:

	G		V
$1, 4; R7;$	$R23$	$3, 4; N7;$	$R23$
$(1, 0, 161)$	$= K$	$(3, 1, 54)$	$= E$
$(9, 1, 18)$	$= 2E$	$(6, -1, 27)$	$= 3E$
$(2, 1, 81)$	$= 4E$	$(6, 1, 27)$	$= 5E$
$(9, -1, 18)$	$= 6E$	$(3, -1, 54)$	$= 7E$

	V'		V''
$3, 4; R7;$	$N23$	$1, 4; N7;$	$N23$
$(7, 0, 23)$	$= A$	$(10, 3, 17)$	$= A + E$
$(11, -2, 15)$	$= A + 2E$	$(5, 2, 33)$	$= A + 3E$
$(14, 7, 15)$	$= A + 4E$	$(5, -2, 33)$	$= A + 5E$
$(11, 2, 15)$	$= A + 6E$	$(10, -3, 17)$	$= A + 7E$

Donada una classe de formes, Gauss considera el seu grup d'isotropia que, en el cas binari, només depèn del discriminant. Veu que la solució general per a representar un nombre representable per una classe prové d'una solució particular modificada amb les representacions que en resulten per l'acció del grup d'isotropia. Alhora, el grup d'isotropia de la forma es calcula resolent una equació de Pell-Fermat. Calcula la solució particular més petita de l'equació de Pell-Fermat i, en tenir en compte l'estructura general de les solucions d'aquesta equació, n'obté la solució general.

En el cas binari considerat per Gauss, cada gènere de formes conté el mateix nombre de classes. Les lleis de composició no només estan definides per a les classes, sinó que es poden definir també per als gèneres. La composició es fa de manera que si una forma representa un nombre i una altra un altre, la composició representa el producte.

La distinció dels diferents gèneres per mitjà de caràcters originà més endavant la definició de l'anomenat caràcter de Kronecker. Com que Gauss no pot donar fórmules generals per al nombre de classes, es dedica a estudiar molts exemples. A les *Disquisicions* ens diu que quan el llibre es va imprimir havia calculat el nombre de classes fins a $D = -3000$. Aleshores es dedicà a estudiar quins discriminants

proporcionen un determinat nombre de classes i a formular conjectures sobre el seu comportaments asimptòtic. Les conjectures de Gauss sobre els nombres de classes han estat fonts de treball fins avui.

> El primer nombre, romà, indica la quantitat de gèneres pròpiament primitius i positius; el següent, la quantitat de classes contingudes en cada gènere; després la sèrie de determinants a què correspon aquella classificació i dels quals s'omet, per a abreujar, el signe negatiu.
>
> $I.\ 1 \ldots, 1, 2, 3, 4, 7.$
> $I.\ 3 \ldots, 11, 19, 23, 27, 31, 43, 67, 163.$
> $I.\ 5 \ldots, 47, 79, 103, 127.$
> $I.\ 7 \ldots, 71, 151, 223, 343, 463, 487.$
> $II.\ 1 \ldots, 5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58.$
> $II.\ 2 \ldots, 14, 17, 20, 32, 34, 36, 39, 46, 49, 52, 55, 63, 64,$
> $\quad 73, 82, 97, 100, 142, 148, 193.$
> $\ldots$
> $XVI.\ 1 \ldots, 840, 1320, 1365, 1848.$

Denotem per $H(D)$ el grup de classes de formes quadràtiques binàries de discriminant D. L'estudi de Gauss dels ordres equival a l'estudi dels subanells $\mathcal{O}(D_0 f^2)$ continguts en el cos quadràtic $\mathbb{Q}(\sqrt{D_0})$, on D_0 denota un discriminant fonamental. L'estudi del grup de classes $H(D_0 f^2)$ equival al del grup de classes d'ideals invertibles d'aquests anells. El grup dels gèneres es remet a l'estudi dels grups quocient $H(D)/H(D)^2$. Els caràcters defineixen el grup dual d'aquests grups.

En aquesta secció, l'estudi dels gèneres de les formes quadràtiques permet a Gauss donar una segona demostració del teorema fonamental.

Anys després, Gauss empraria de nou les formes quadràtiques binàries, però en el seu estudi de la curvatura de les superfícies.

Secció sisena. Aplicacions diverses de les disquisicions precedents

Aquesta és una secció força breu. Té 49 pàgines.

Gauss aplica alguns resultats de les seccions anteriors a l'estudi de les qüestions següents:

• Descomposició de fraccions en fraccions més simples. Per exemple,

$$\frac{391}{924} = \frac{1}{4} + \frac{2}{3} + \frac{1}{7} + \frac{4}{11} - 1.$$

• Conversió de fraccions en fraccions decimals.

• Aplicacions dels mètodes precedents i de les formes quadràtiques binàries a l'estudi de problemes de divisibitat en els enters.

Aquesta darrera aplicació és per a Gauss especialment important:

> El problema de distingir nombres primers de compostos i descompondre aquests en els seus factors primers, que pertany als més importants i més útils de tota l'aritmètica [...].

No deixa de sorprendre que Gauss digui, l'any 1801, que descompondre un nombre en factors primers i distingir els nombres primers dels compostos sigui un dels problemes més útils de tota l'aritmètica. No sé quina podia ser l'aplicació pràctica d'aquestes tècniques a l'època de Gauss. En la nostra, en canvi, la utilitat d'aquests coneixements és palesa en els mètodes criptogràfics de clau pública. Com és sabut, la seguretat d'aquests mètodes es basa en la complexitat de la factorització dels nombres enters en producte de primers o en la complexitat del logaritme discret. No cal dir que recursos continguts a les *Disquisicions* han estat utilitzats en innombrables algoritmes criptogràfics. Així, les propietats de l'indicador d'Euler són emprades en el popular protocol RSA, el logaritme discret és emprat en el protocol ElGamal i les formes ambigües són emprades en alguns mètodes de factorització.

Secció setena. De les equacions que defineixen les seccions del cercle

La darrera secció té 71 pàgines. Torna a ser una secció absolutament brillant.

Gauss tracta aquí el problema de la divisió de la circumferència en parts iguals; equivalentment, estudia el problema de la caracterització dels polígons regulars que són construïbles amb regla i compàs, un problema heretat de l'Antiguitat grega.

Tota la secció constitueix un precedent de la teoria de Galois. Si expressem els resultats de Gauss en el llenguatge d'aquesta, podem dir que Gauss determina, donat un nombre primer p, tots els subgrups del grup de Galois del cos de les arrels p-èsimes de la unitat i tots els subcossos fixos per a aquests subgrups. Dels subcossos en proporciona elements primitius explícits per mitjà dels períodes de les equacions ciclotòmiques.

Atès que les *Disquisicions* foren traduïdes al francès quatre anys abans que Galois naixés, és evident que l'obra de Gauss pogué influir en les idees de Galois. Els treballs de Galois per a la caracterització de les equacions resolubles per radicals esdevenen la continuació natural de l'anàlisi que porta a terme Gauss en aquesta secció sobre les arrels de les equacions que defineixen les seccions del cercle. Aquesta influència de Gauss en Galois, però, no se sol esmentar. Només n'he trobat una breu referència en Klein [Kl1925].

La principal diferència tècnica entre la teoria de Galois i el contingut d'aquesta secció es troba en el fet que en l'estudi de les equacions ciclotòmiques només intervenen grups abelians. Així, si bé a l'obra de Gauss ja s'hi troben implícits conceptes com el de grup, subgrup, quocients, etc., Gauss no necessita el concepte de subgrup normal.

Per a demostrar els resultats esmentats sobre les seccions del cercle, Gauss utilitzarà resultats de les primeres seccions. Trobem així, per primera vegada, connexions entre la teoria de Galois i l'aritmètica.

> Parlo de la teoria de les funcions trigonomètriques corresponents a arcs commensurables amb la perifèria, o sigui, de la teoria dels polígons regulars, [...] el mateix tractament mostrarà suficientment que entre aquesta qüestió i l'aritmètica superior hi ha inherent un nexe íntim.

Gauss dóna la llista dels primers polígons que són construïbles amb regle i compàs. No es limita únicament a aquells que tenen un nombre primer de costats (i que, per tant, són de la forma $p = 2^m + 1$, és a dir, 2, 3, 5, 17, 257, 65537,...), sinó que els hi inclou tots (és a dir, els nombres que són producte de primers diferents de la forma anterior per potències de 2):

$$2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32,$$
$$34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 128,$$
$$136, 160, 170, 192, 204, 240, 255, 256, 257, 272, \ldots$$

En la secció XIII dels *Elements*, Euclides havia deduït fórmules equivalents a les següents, on ℓ_n denota la longitud del costat del polígon regular de n costats inscrit en la circumferència de radi unitat i L_n denota la longitud de l'aresta del políedre regular de n cares inscrit a

l'esfera de radi unitat:

$$\begin{aligned}
\ell_3 &= \sqrt{3}, \\
\ell_4 &= \sqrt{2}, \\
\ell_5 &= \tfrac{1}{2}\sqrt{10-2\sqrt{5}}, \\
\ell_6 &= 1, \\
\ell_{10} &= \tfrac{1}{2}(\sqrt{5}-1);
\end{aligned}$$

$$\begin{aligned}
L_4 &= \tfrac{2}{3}\sqrt{6}, \\
L_6 &= \tfrac{2}{3}\sqrt{3}, \\
L_8 &= \sqrt{2}, \\
L_{12} &= \tfrac{\sqrt{3}}{3}(\sqrt{5}-1), \\
L_{20} &= \tfrac{1}{5}\sqrt{10(5-\sqrt{5})}.
\end{aligned}$$

Com que en les magnituds anteriors només hi intervenen arrels quadrades, deduïm que totes elles són construïbles fent ús únicament del regle i del compàs.

La fórmula que segueix, deguda a Gauss, proporciona $\cos(2\pi/17)$ com una expressió en la qual intervenen únicament radicals quadràtics. Per tant, la fórmula mostra que el polígon de 17 costats és construïble amb regle i compàs i, alhora, proporciona un mètode per a realitzar-ne la construcció.

Per a $n = 17$, dels articles 354, 361, es deriva fàcilment l'expressió

$$\begin{aligned}
\cos\frac{2\pi}{17} &= -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34-2\sqrt{17}} \\
&\quad + \frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}.
\end{aligned}$$

És realment sorprenent en gran manera que, encara que la divisibilitat geomètrica del cercle en tres i cinc parts ja fos coneguda des del temps d'Euclides, no s'hagi afegit res a aquests descobriments en l'interval de 2000 anys.

En el que segueix, explicarem la deducció de Gauss de la fórmula anterior, però traduïda en termes i notació actuals.

Donat un nombre primer p, considerem l'arrel primitiva p-èsima de la unitat

$$\zeta_p := e^{2\pi i/p}.$$

Sigui $n := \varphi(p) = p-1$ el valor de l'indicador d'Euler en p. Per al grup de Galois de l'extensió $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, es té que

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^*.$$

Atesa l'existència d'arrels primitives mòdul p, $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ és una extensió cíclica. Sigui g una arrel primitiva mòdul p; és a dir,

$$(\mathbb{Z}/p\mathbb{Z})^* = (g).$$

Escrivim $\mathrm{G}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = (\sigma)$, on σ és l'automorfisme definit segons

$$\sigma(\zeta_p) := \zeta_p^g.$$

Aleshores, se satisfà la proposició següent:

Proposició.

(i) *Per a cada divisor f de n, el grup (g) admet un únic subgrup d'ordre f, també cíclic:*

$$(g^e) = \{g^e, g^{2e}, ..., g^{fe}\},$$

on $fe = n$.

(ii) *Per a cada divisor f de $p-1$, existeix un subcòs $K \subseteq \mathbb{Q}(\zeta_p)$, únic, tal que $[\mathbb{Q}(\zeta_p) : K] = f$ i, a més,*

$$\mathrm{G}(\mathbb{Q}(\zeta_p)/K) = (\sigma^e).$$

Passem ara al càlcul del cos $K = \mathbb{Q}(\zeta_p)^{(\sigma^e)}$, és a dir, del cos fix per (σ^e). Les $\varphi(p) = n$ arrels primitives p-èsimes de 1 són

$$\zeta_p^g, \zeta_p^{g^2}, ..., \zeta_p^{g^n} = \zeta_p.$$

Definim, d'acord amb Gauss, un símbol

$$[m] := \zeta^{g^m}.$$

Amb aquests símbols s'opera com a $\mathbb{Z}/n\mathbb{Z}$, atès que

$$[m+n] = \zeta^{g^{m+n}} = \zeta^{g^m} = [m].$$

De manera natural, el grup $\mathrm{G}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ opera en els símbols per translacions, d'acord amb:

$$\begin{aligned}\sigma[m] &= \sigma(\zeta_p^{g^m}) = \sigma(\zeta_p)^{g^m} = (\zeta^g)^{g^m} = [m+1],\\ \sigma^j[m] &= [m+j].\end{aligned}$$

Fixat un divisor f de n, considerem els elements

$$\eta_k := [k] + [k+e] + [k+2e] + [k+3e] + ... + [k+(f-1)e].$$

Per definició, els elements η_k són els períodes f-èsims del cos ciclotòmic $\mathbb{Q}(\zeta_p)$.

Teorema. *Sigui $ef = p-1$. Aleshores,*

$$\mathbb{Q}(\eta_0) = ... = \mathbb{Q}(\eta_{e-1}), \qquad \mathrm{G}(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\eta_k)) = (\sigma^e).$$

Demostració. Els elements $1, \zeta, ..., \zeta^{p-2}$ són $\mathbb{Q}$-linealment independents. Alhora, els elements

$$[1], [2], ..., [n] = [p-1]$$

són $\mathbb{Q}$-linealment independents. De

$$\sigma^j[\eta_k] = [k+j] + [k+e+j] + ... + [k+(f-1)e+j]$$

se segueix que $\sigma^j[\eta_k] = [\eta_k]$ si, i només si, $j = \lambda e + \mu(p-1)$ si, i només si, e divideix j o bé, equivalentment, $\sigma^j \in (\sigma^e)$. □

Per a arribar a la fórmula del $\cos(2\pi/17)$, prenem $p = 17$ i particularitzem els càlculs anteriors en els divisors de 16.

• Càlcul dels períodes per a $p = 17$

Siguin $\vartheta := \dfrac{2\pi}{17}$, $\zeta = \zeta_{17}$. Es té que

$$\mathrm{G}(\mathbb{Q}(\zeta_{17})/\mathbb{Q}) \simeq (\mathbb{Z}/17\,\mathbb{Z})^* = (3);$$

més precisament,

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^m	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

(i) Cas $f = 8$ i $e = 2$

Tenim dos 8-períodes a $\mathbb{Q}(\zeta_{17})$:

$$\begin{aligned}\eta_0 &= [0]+[2]+[4]+[6]+[8]+[10]+[12]+[14]\\ &= \zeta+\zeta^9+\zeta^{13}+\zeta^{15}+\zeta^{16}+\zeta^8+\zeta^4+\zeta^2\\ &= 2(\cos\alpha+\cos 8\alpha+\cos 4\alpha+\cos 2\alpha),\\ \eta_1 &= [1]+[3]+[5]+[7]+[9]+[11]+[13]+[15]\\ &= \zeta^3+\zeta^{10}+\zeta^5+\zeta^{11}+\zeta^{14}+\zeta^7+\zeta^{12}+\zeta^6\\ &= 2(\cos 3\alpha+\cos 7\alpha+\cos 5\alpha+\cos 6\alpha).\end{aligned}$$

La suma de totes les arrels d'ordre 17 de la unitat és -1. Per tant,

$$\eta_0+\eta_1=-1.$$

Tenint present la fórmula

$$2\cos(k\alpha)\cos(l\alpha)=\cos((k+l)\alpha)+\cos((k-l)\alpha),$$

obtenim que

$$\eta_0\,\eta_1=4(\eta_0+\eta_1)=-4.$$

Així, els 8-períodes coincideixen amb les arrels de l'equació

$$X^2+X-4=0;$$

és a dir,

$$\eta_0=\frac{-1+\sqrt{17}}{2},\qquad \eta_1=\frac{-1-\sqrt{17}}{2},$$

tal com es dedueix un cop feta la identificació de les arrels. Per tal de distingir les arrels, notem que totes dues són reals; una és positiva i l'altra, negativa. Però

$$\cos\alpha+\cos 2\alpha>2\cos\frac{\pi}{4}=\sqrt{2}>-\cos 8\alpha$$

$\cos 4\alpha>0$, per tant $\eta_0>0$. Així $\eta_0>\eta_1$, d'acord amb l'elecció feta.

(ii) Cas $f=4$, $e=4$

Tenim quatre 4-períodes a $\mathbb{Q}(\zeta_{17})$:

$$\lambda_0=[0]+[4]+[8]+[12],\quad \lambda_1=[1]+[5]+[9]+[13],$$

$$\lambda_2=[2]+[6]+[10]+[14],\quad \lambda_3=[3]+[7]+[11]+[15].$$

λ_0, λ_2 són les arrels de l'equació

$$X^2 - \eta_0 X - 1 = 0,$$

λ_1, λ_3 són les arrels de l'equació

$$X^2 - \eta_1 X - 1 = 0.$$

(iii) Cas $f = 2$, $e = 8$

Tenim vuit 2-períodes a $\mathbb{Q}(\zeta_{17})$. Escrivim-ne dos:

$$\mu_0 = [0] + [8], \quad \mu_1 = [4] + [12].$$

μ_0, μ_1 són les arrels de l'equació $X^2 - \lambda_0 X + \lambda_1 = 0$.

(iv) Cas $f = 1$, $e = 16$

Arribem a ζ, atès que se satisfà

$$\zeta + \zeta^{-1} = \mu_0 = 2\cos\alpha, \quad \zeta\zeta^{-1} = 1.$$

D'aquesta manera, obtenim la cadena descendent de subcossos:

$$\mathbb{Q}(\zeta_{17}) \supseteq \mathbb{Q}(\mu_0) \supseteq \mathbb{Q}(\lambda_0) \supseteq \mathbb{Q}(\eta_0) \supseteq \mathbb{Q}.$$

La fórmula cercada,

$$\begin{aligned}\cos\frac{2\pi}{17} &= -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} \\ &\quad + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}},\end{aligned}$$

s'obté per substitucions successives de tots els períodes calculats.

Gauss suggereix que la teoria exposada en aquesta secció s'estén més enllà de l'estudi de les seccions del cercle.

> Els principis de la teoria [...] no només es poden aplicar a les funcions circulars, sinó, amb èxit semblant, a moltes altres funcions transcendents, per exemple, a les que depenen de la integral
>
> $$\int \frac{dx}{\sqrt{1 - x^4}}.$$

FIGURA 5. Monument a C. F. Gauss i a W. Weber, a Gotinga

La indicació de Gauss fou treballada per Abel. Abel amplià el mètode de Gauss exposat en aquesta secció a la determinació de les seccions de la lemniscata construïbles amb regle i compàs. Les recerques d'Abel proporcionaren extensions galoisianes de cossos quadràtics amb grup de Galois també commutatiu, és a dir *abelià*. Els resultats d'Abel en aquest context donaren lloc a la teoria de la multiplicació complexa.

Resum de les Disquisicions

Poden resumir el contingut de les *Disquisicions* de la manera següent.

Seccions 1, 2, 3, 6: Destinades a recopilar coneixements de l'època, donaren lloc a estudis posteriors relatius a grups abelians, cossos finits, àlgebra lineal, nombres primers, factorització, etc.

S'hi tracten les equacions de congruència

$$ax + b \equiv c \pmod{m}, \quad x^m \equiv a \pmod{p}.$$

Secció 4: Conté la llei de reciprocitat quadràtica. Aquest capítol motivà l'estudi posterior de les lleis de reciprocitat associades a extensions abelianes de cossos de nombres.

S'hi tracten les equacions de congruència quadràtiques

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

Secció 5: Conté l'estudi de les formes quadràtiques binàries i de les formes quadràtiques ternàries de coeficients enters. Més endavant, motivà l'estudi aritmètic dels cossos de nombres, la creació de la teoria d'ideals, l'estudi dels anells de Dedekind, l'estudi de formes de grau superior, dels comportaments asimptòtics dels nombres de classes, etc. Alhora, el capítol motivà estudis posteriors de geometria hiperbòlica, lligats a accions de grups discrets de transformacions del pla.

S'hi tracten les equacions

$$ax^2 + 2bxy + cy^2 = d.$$

Secció 7: El seu contingut equival a l'estudi de les equacions ciclotòmiques. Constitueix un precedent de la teoria de Galois. Donà peu a l'estudi de les funcions el·líptiques, teoria de la multiplicació complexa, etc.

S'hi tracten les equacions

$$x^p - 1 = 0.$$

Per acabar, esmentem algunes entrades extretes del *Diari de Gauss* [1796-1814] per la seva relació amb el contingut de les *Disquisicions*.

[1, 1796] Principis en què es basa la divisió del cercle, i divisió geomètrica d'aquest en 17 parts, etc.

[62, 1797] La lemniscata és divisible geomètricament en cinc parts.

[84, 1798] En un ordre qualsevol s'hi troben classes, i d'ací es redueix a una teoria sòlida la representabilitat dels nombres com a tres quadrats.

[96, 1799] Hem començat a considerar formes d'ordre més gran.

[103, 1800] Èxit en la determinació de les formes reduïdes en la teoria de les formes ternàries.

[140, 1809] Hem acabat la divisió per cinc fent servir la mitjana aritmètico-geomètrica.

[144, 1813] La fonamentació de la teoria general dels residus biquadràtics, que havíem estat cercant amb el màxim esforç durant gairebé set anys, endebades, ha estat descoberta, a la fi, el mateix dia que naixia el nostre fill.

Referències

[Bu1981] Buhler, W. K.: *Gauss: a biographical study*. Springer, 1981.

[Ga1996] Gauss, C. F.: *Disquisicions aritmètiques*. Carl Friedrich Gauss. Traducció i pròleg de Griselda Pascual Xufré, 1996. XXVIII+654 p. Societat Catalana de Matemàtiques. ISBN 84-7283-313-5. Primera edició: *Disquisitiones arithmeticæ*. Lipsiæ, Fleischer, 1801.

[Kl1925] Klein, F.: *Entwicklung der Mathematik im 19. Jahrhundert* I. Berlin, 1925. http://books.google.com.

[Le1798] Legendre, A. M.: *Essai sur une théorie des nombres*. Paris. Duprat, 1798. http://books.google.com

[Lem2000] Lemmermeyer, F.: *Reciprocity Laws, from Euler to Eisenstein*. Springer, 2000.

[Ne1992] Neukirch, J.: *Algebraische Zahlentheorie*. Springer, 1992.

[Se1973] Serre, J-P.: *A course in Arithmetic*. Springer, GTM 7, 1973.

[Tr1998] Travesa, A.: *Aritmètica*. Col·lecció UB, 25. Edicions de la Universitat de Barcelona, 1998.

[Za1981] Zagier, D.: *Zetafunktionen und quadratische Körper*: *eine Einführung in die höhere Zahlentheorie*. Springer, 1981.