# GAUSS and the cyclotomic equation *

HENRIK KRAGH SØRENSEN
History of Science Department
University of Aarhus, Denmark
hkragh@imf.au.dk

3rd March 2001

Thirty years after LAGRANGE's creative studies on known solutions to low degree equations, and in particular properties of rational functions under permutations of their arguments, another great master published a work of profound influence on early $19^{th}$ century mathematics. From his position in Göttingen, C. F. GAUSS was located at a physical distance from the emerging centers of mathematical research in Paris and Berlin. By 1801, the Parisian mathematicians had for some time been publishing their results in French — and, within a generation, the German mathematicians would also be writing in their paternal language, at least for publications intended for AUGUST LEOPOLD CRELLE's (1780–1855) *Journal für die reine und angewandte Mathematik*. But when GAUSS published his *Disquisitiones arithmeticae* (1801), it was written in Latin and published as a monograph as was still customary to his generation of German scholars.

The book was divided into seven sections, although allusions and references were made to an eighth section which GAUSS was never to complete for publication[1]. The main part was concerned with the theory of congruences, the theory of forms, and related number theoretic investigations. Together, these topics provided a new foundation, emphasis, and disciplinary independence — as well as a wealth of results — for $19^{th}$ century number theorists — in particular GUSTAV PETER LEJEUNE DIRICHLET (1805–1859) — to elaborate. In dealing with the classification of forms, GAUSS made use of "implicit group theory"[2] but the abstract concept of groups was almost as far beyond GAUSS as it had been beyond LAGRANGE.

One of the new tools applied by GAUSS in the theory of congruences was that of *primitive roots*. In the articles 52–57, GAUSS gave his exposition of EULER's treatment of primitive roots. A primitive root $k$ of modulus $\mu$ is an integer $1 < k < \mu$ such that the set of remainders of its powers $k^1, k^2, \ldots, k^{\mu-1}$ modulo $\mu$ coincides with the set

*This is a revised excerpt from my progress report (November 1999).

[1](Gauss *Werke*, vol. 1, 477). It is, however, included among the *Nachlass* in the second volume of the *Werke* (Gauss *Werke*).

[2](Wussing 1969, 40–44).

$\{1, 2, \ldots, \mu - 1\}$, possibly in a different order. A central result obtained was the existence of $p - 1$ different primitive roots of modulus $p$ if $p$ were assumed to be prime.

# 1 The division problem for the circle

In the seventh section of his *Disquisitiones arithmeticae* (1801), GAUSS turned his investigations toward the equations defining the division of the periphery of the circle into equal parts. He was interested in the ruler–and–compass constructibility[3] of regular polygons and was therefore led to study in details *how*, i.e. by the extraction of which roots, the binomial equations of the form

$$x^n - 1 = 0 \tag{1}$$

could be solved algebraically. If the roots of this equation could be constructed by ruler and compass, then so could the regular $p$-gon. It is evident from GAUSS' mathematical diary that this problem had occupied him from a very early stage in his mathematical career and had been the deciding factor in his choice of mathematics over classical philology[4]. The very first entry in his mathematical progress diary from 1796 read:

> "[1] The principles upon which the division of the circle depend, and geometrical divisibility of the same into seventeen parts, etc. [1796] March 30 Brunswick." (Gray 1984, 106)[5]

In his introductory remarks of the seventh section, GAUSS noticed that the approach which had led him to the division of the circle could equally well be applied to the division of other transcendental curves of which he gave the lemniscate as an example.

> "The principles of the theory which we are going to explain actually extend much farther than we will indicate. For they can be applied not only to circular functions but just as well to other transcendental functions, e.g. to those which depend on the integral $\int [1/\sqrt{(1 - x^4)}]\, dx$ and also to various types of congruences." (Gauss 1986, 407)[6]

However, as he was preparing a treatise on these topics GAUSS had chosen to leave this extension out of the *Disquisitiones*. GAUSS never wrote the promised treatise, and

[3] In the following I refer to *Euclidean construction*, i.e. by ruler and compass when I speak of *constructions* or *constructibility*.

[4] (Biermann 1981, 16).

[5] "*[1.] Principia quibus innititur sectio circuli, ac divisibilitas eiusdem geometrica in septemdecim partes etc. [1796] Mart. 30. Brunsv[igae]*" (Gauss 1981, 21, 41)

[6] "*Ceterum principia theoriae, quam exponere aggredimur, multo latius patent, quam hic extenduntur. Namque non solum ad functiones circulares, sed pari successu ad multas functiones transscendentes applicari possunt, e.g. ad eas, quae ab integrali* $\int \frac{\mathrm{d}x}{\sqrt{(1-x^4)}}$ *pendent, praetereaque etiam ad varia congruentiarum genera.*" (Gauss 1801, 412–413)

after ABEL had published his first work on elliptic functions (Abel 1827) culminating in the division of the lemniscate, GAUSS gave him credit for carrying these investigations into print[7].

A first simplification of the study of the constructibility of a regular $n$-gon was made when GAUSS observed that he needed only to consider cases in which $n$ was a prime since any polygon with a composite number of edges could be constructed from the polygons with the associated prime numbers of edges. Individual equations expressing the sine, the cosine, and the tangent were well known, but none of those were as suitable for GAUSS' purpose as the equation $x^n - 1 = 0$ of which he knew that the roots were[8]

$$\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = 1 \text{ when } 0 \leq k \leq n-1.$$

Inspecting these roots, GAUSS observed that the equation $x^n - 1 = 0$ for odd $n$ had a single real root, $x = 1$, and the remaining imaginary roots were all given by the equation

$$X = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \ldots + x + 1 = 0, \tag{2}$$

the roots of which GAUSS thought of as forming the *complex* $\Omega$. When GAUSS used the term "complex" (Latin: *complexum*) he thought of it as a collection of objects (here roots) without any structure imposed. Initially, GALOIS used the French term *groupe* in a similar (naive) way before it later gradually acquired its status as a mathematical term[9]. The evolution of everyday words into mathematical concepts is a characteristic of the early $19^{th}$ century and is dealt with in chapter **??**. GAUSS then demonstrated that if $r$ designated any root in $\Omega$, all roots of (1) could be expressed as powers of $r$, thereby saying that any root in $\Omega$ was a primitive $n^{th}$ root of unity.

## 2 Irreducibility of the equation $\frac{x^n-1}{x-1} = 0$

An interesting feature of GAUSS' approach was his focusing on the *system* or *complex* of roots instead of the individual roots. This slight shift in the conception of roots enabled GAUSS (as it had enabled LAGRANGE) to study properties of the equations which could only be captured in studies of the entire system of roots. To GAUSS, the most important property was that of *decomposability* or *irreducibility*. In article 341, GAUSS demonstrated through an *ad hoc* argument that the function $X$ (2) could not be decomposed into polynomials of lower degree with rational coefficients. In modern terminology, he proved that the polynomial $X$ was irreducible over $\mathbb{Q}$.

GAUSS' proof assumed that the function

$$X = x^{n-1} + x^{n-2} + \ldots + x + 1$$

[7](A. L. Crelle→N. H. Abel, 1828. In Abel *Breve*, 62).

[8]GAUSS wrote $P$ (periphery) for $2\pi$, but the use of $i$ for $\sqrt{-1}$ is his.

[9](Wussing 1969, 78).

was divisible by a function of lower degree

$$P = x^{\lambda} + Ax^{\lambda-1} + Bx^{\lambda-2} + \ldots + Kx + L, \tag{3}$$

in which the coefficients $A, B, \ldots, K, L$ were rational numbers. Assuming $X = PQ$ GAUSS introduced the two systems of roots $\mathfrak{P}$ and $\mathfrak{Q}$ of $P$ and $Q$ respectively. From these two systems GAUSS defined another two consisting of the reciprocal roots[10]

$$\hat{\mathfrak{P}} = \left\{r^{-1} : r \in \mathfrak{P}\right\} \text{ and } \hat{\mathfrak{Q}} = \left\{r^{-1} : r \in \mathfrak{Q}\right\}.$$

Although GAUSS consistently termed the roots of $\hat{\mathfrak{P}}$ and $\hat{\mathfrak{Q}}$ *reciprocal roots*, it is easy for us to see that they are what we would term *conjugate roots* since any root in $\mathfrak{P}$ has unit length.

The subsequent argument was split into four different cases. The opening one is the most interesting one, namely the case in which $\mathfrak{P} = \hat{\mathfrak{P}}$, i.e. when all roots of $P = 0$ occur together with their conjugates. It may appear strange that GAUSS considered other cases as we know perfectly well that in any polynomial with real coefficients the imaginary roots occur in conjugate pairs[11]. After observing that $P$ was the product of $\frac{\lambda}{2}$ paired factors of the form

$$(x - \cos\omega)^2 + \sin^2\omega,$$

GAUSS concluded that these factors would assume real and positive values for all real values of $x$, which would then also apply to the function $P(x)$. He then formed $n-1$ auxiliary equations[12]

$$P^{(k)} = 0 \text{ where } 1 \leq k \leq n-1$$

defined by their root systems $\mathfrak{P}^{(k)}$ consisting of $k^{th}$ powers of the roots of $P = 0$,

$$\begin{aligned} \mathfrak{P}^{(k)} &= \left\{r^k : r \in \mathfrak{P}\right\}, \\ P^{(k)}(x) &= \prod_{s \in \mathfrak{P}^{(k)}} (x - s) = \prod_{r \in \mathfrak{P}} \left(x - r^k\right). \end{aligned}$$

Following the introduction of the numbers $p_k$ defined by

$$p_k = P^{(k)}(1) = \prod_{s \in \mathfrak{P}^{(k)}} (1 - r) = \prod_{r \in \mathfrak{P}} \left(1 - r^k\right),$$

[10] The notation $\hat{\mathfrak{P}}$ and $\hat{\mathfrak{Q}}$ for these is mine.

[11] JOHNSEN has argued (1984) that this apparently unnecessary complication in GAUSS' argument can be traced back to a more general concept of irreducibility over fields different from $\mathbb{Q}$, for instance the field $\mathbb{Q}(i)$. If so, there are no explicit hints at such a concept in the *Disquisitiones* and the result which GAUSS proved only served a very specific purpose in his larger argument, and did not give a general concept, general criteria, or a body of theorems concerning irreducibility over $\mathbb{Q}$ or any other field. The proof relies more on number theory (higher arithmetic) than on general theorems and criteria concerning irreducible equations, let alone any general concept of fields distinct from the rational numbers $\mathbb{Q}$.

[12] The notation $P^{(k)}$ and $\mathfrak{P}^{(k)}$ is mine.

GAUSS used properties derived in a previous article, 340, to establish

$$\sum_{k=1}^{n-1} p_k = \sum_{k=1}^{n-1} P^{(k)}(1) = nA. \tag{4}$$

Furthermore,

$$\begin{aligned} \prod_{k=1}^{n-1} P^{(k)}(x) &= \prod_{k=1}^{n-1}\prod_{r\in\mathfrak{P}}\left(x - r^k\right) = \prod_{r\in\mathfrak{P}}\prod_{k=1}^{n-1}\left(x - r^k\right) = \prod_{r\in\mathfrak{P}} X = X^\lambda, \text{ and} \\ \prod_{k=1}^{n-1} p_k &= \prod_{k=1}^{n-1} P^{(k)}(1) = X^\lambda(1) = n^\lambda \text{ since } X(1) = n. \end{aligned}$$

From the article 338 which dealt with constructing an equation with the $k^{th}$ powers of the roots of a given equation as its roots, GAUSS knew that the coefficients of $P^{(1)}, \ldots, P^{(n-1)}$ would be rational numbers if the coefficients of $P$ were rationals. Much earlier, in article 42, he had furthermore demonstrated that the product of two polynomials with rational but not integral coefficients could not be a polynomial with integral coefficients. Since $X$ had integral coefficients and $P$ had rational coefficients by assumption, it followed that the coefficients of $P^{(1)}, \ldots, P^{(n-1)}$ would indeed be integers, since any $P^{(k)}$ was a factor of $X^\lambda$ with rational coefficients. Consequently, the quantities $p_k$ would have to be integral, and since their product was $n^\lambda$ and there were $n - 1 > \lambda$ of them, at least $n - 1 - \lambda$ of the quantities $p_k$ would have to be equal to $1$ and the others would have to equal $n$ or some power of $n$ since $n$ was assumed to be prime. But if the number of quantities equal to $1$ was $g$ it would follow that

$$\sum_{k=1}^{n-1} p_k \equiv g \pmod{n},$$

which GAUSS saw would contradict (4) since $0 < g < n$.

The other cases, which in the presently adopted notation can be described as

2. $\mathfrak{P} \neq \hat{\mathfrak{P}}$ and $\mathfrak{P} \cap \hat{\mathfrak{P}} \neq \emptyset$,
3. $\mathfrak{Q} \cap \hat{\mathfrak{Q}} \neq \emptyset$, and
4. $\mathfrak{P} \cap \hat{\mathfrak{P}} = \emptyset$ and $\mathfrak{Q} \cap \hat{\mathfrak{Q}} = \emptyset$,

could all be brought to a contradiction, either directly or by referring to the first case described above.

The use of the proof of the irreducibility of $X$ was that it demonstrated that if $X$ was decomposed into factors of lower degrees (such as 3) some of these had to have irrational coefficients. Thus any attempt at determining the roots would have to involve equations of degree higher than one. The purpose of the following investigation was to gradually reduce the degree of these equations to minimal values by refining the system of roots.

# 3 Outline of GAUSS's proof

Continuing from the statement above that any root $r$ in $\Omega$ was a primitive $n^{th}$ root of unity, GAUSS wrote $[1], [2], \ldots, [n-1]$ for the associated powers of $r$. He then introduced the concept of periods by defining the *period* $(f, \lambda)$ to be the set of the roots $[\lambda], [\lambda h], \ldots, \left[\lambda h^{f-1}\right]$, where $f$ was an integer such that $n - 1 = ef$, $\lambda$ an integer not divisible by $n$, $g$ a primitive root of the modulus $n$, and $h = g^e$. Connected to the period, he introduced the *sum of the period*, which he also designated $(f, \lambda)$,

$$(f, \lambda) = \sum_{k=0}^{f-1} \left[\lambda h^k\right],$$

and the first result, which he stated concerning these periods, were their independence of the choice of $g$.

Throughout the following argument, GAUSS let $g$ designate a primitive root of modulus $n$ and constructed a sequence of equations through which the periods $(1, g)$, i.e. the roots in $X = 0$ (2), could be determined. Assuming that the number $n - 1$ had been decomposed into primes as

$$n - 1 = \prod_{k=1}^{u} p_k,$$

GAUSS partitioned the roots of $\Omega$ into $\frac{n-1}{p_1}$ periods, each of $p_1$ terms. From these, he formed $p_1$ equations $X' = 0$ having the $\frac{n-1}{p_1}$ sums of the form $(p_1, \lambda)$ as its roots. By a central theorem proved in article 350 using symmetric functions, he could prove that the coefficients of these latter equations depended upon the solution of yet another equation of degree $p_1$. Thus the solution of the original equation of degree $n$ had been reduced to solving $p_1$ equations $X' = 0$ each of degree $\frac{n-1}{p_1}$ and a single equation of degree $p_1$. By repeating the procedure, the equation $X' = 0$ could be solved by solving $p_2$ equations of degree $\frac{n-1}{p_1 p_2}$ and a single equation of degree $p_2$, and the procedure could be iterated further until the solution of the equation $X = 0$ of degree $n - 1$ had been reduced to solving $u$ equations of degrees $p_1, p_2, \ldots, p_u$ since the other equations would ultimately have degree 1.

A special case emerged if $n - 1$ was a power of 2. It was well known that square roots could always be constructed by ruler and compass. Therefore, if $n$ had the form

$$n = 1 + 2^k,$$

the construction of the roots of (1) could be carried out by ruler and compass. By applying this to $k = 4$, GAUSS demonstrated that the regular 17-gon could be constructed by ruler and compass giving the first new constructible regular polygon since the time of EUCLID ($\sim$295BC)[13].

[13] GAUSS, himself, was very aware of the progress he had made, see (Gauss 1986, 458) and (Schneider 1981, 38–39).

By the argument he had described in order to consider only prime $n$'s, GAUSS could also conclude that the construction of the regular $n$-gon was possible by ruler and compass when $n$ had the form

$$n = 2^m \prod_{k=1}^{h} (1 + 2^{u_k})$$

when $\{u_k\}$ was a set of distinct integers such that $\{1 + 2^{u_k}\}$ were primes, the so-called *Fermat primes*. The converse implication, that only such $n$-gons were constructible, was claimed without detailed proof by GAUSS:

> "Whenever $n - 1$ involves prime factors other than $2$, we are always led to equations of higher degree, namely to one or more cubic equations when $3$ appears once or several times among the prime factors of $n - 1$, to equations of the fifth degree when $n - 1$ is divisible by $5$, etc. **We can show with all rigor that these higher-degree equations cannot be avoided in any way nor can they be reduced to lower-degree equations**. The limits of the present work exclude this demonstration here, but we issue this warning lest anyone attempt to achieve geometric constructions for sections other than the ones suggested by our theory (e.g. sections into $7$, $11$, $13$, $19$, etc. parts) and so spend his time uselessly." (Gauss 1986, 459)[14]

The class of equations (the cyclotomic ones) which GAUSS had demonstrated had constructible roots was also interesting from the point of algebraic solvability of equations. In the argument of his proof, GAUSS had demonstrated that they were indeed solvable by radicals including only square roots, whereby the first new non-elementary class of solvable high-degree equations had been established. By the time GAUSS wrote his *Disquisitiones*, he had come to suspect that not all equations were solvable by radicals, and thus this newly found class was taken as an special example of equations having this nice property. The belief of important mathematicians in the general solvability of equations had, as we shall see, been declining over the $18^{th}$ century, and GAUSS was important in bringing about the ultimate change.

[14] "*Quoties autem $n - 1$ alios factores primos praeter $2$ implicat, semper ad aequationes altiores deferimur; puta ad unam pluresve cubicas, quando $3$ semel aut pluries inter factores primos ipsius $n - 1$ reperitur, ad aequationes quinti gradus, quando $n - 1$ divisibilis est per $5$ etc.,* ***omnique rigore demonstrare possumus, has aequationes elevatas nullo modo nec evitari nec ad inferiores reduci posse****, etsi limites huius operis hanc demonstrationem hic tradere non patiantur, quod tamen monendum esse duximus, ne quis adhuc alias sectiones praeter eas, quas theoria nostra suggerit, e.g. sectiones in $7$, $11$, $13$, $19$ etc. partes, ad constructiones geometricas perducere speret, tempusque inutiliter terat.*" (Gauss 1801, 462) Bold-face has been substituted for small-caps.

# References

Abel, N. H. (1827). Recherches sur les fonctions elliptiques. *Journal für die reine und angewandte Mathematik 2*(2), 101–181.

Abel, N. H. (*Breve*). Breve fra og til Abel. In E. Holst, C. Størmer, and L. Sylow (Eds.), *Festskrift ved Hundredeaarsjubilæet for Niels Henrik Abels Fødsel*. Kristiania: Jacob Dybwad.

Biermann, K.-R. (1981). Historische Einführung. In Gauss (1981), pp. 7–20.

Gauss, C. F. (1801). Disquisitiones arithmeticae. In volume 1 of Gauss (*Werke*), pp. 3–474. First published Leipzig: Gerh. Fleisher. Translated into English in Gauss (1986).

Gauss, C. F. (1981). *Mathematisches Tagebuch 1796–1814*. Number 256 in Ostwalds Klassiker der exakten Wissenschaften. Leipzig: Akademische Verlagsgesellschaft, Geest & Portig K.-G.

Gauss, C. F. (1986). *Disquisitiones Arithmeticae. English Edition*. New York, Berlin, Heidelberg, Tokyo: Springer-Verlag. Edited by A. A. Clarke and W. C. Waterhouse.

Gauss, C. F. (*Werke*). *Carl Friedrich Gauss Werke*. Göttingen: Königlichen Gesellschaft der Wissenschaften. 1863–????. ? vols. Reprinted 1973–???? Hildesheim and New York: Georg Olms Verlag.

Gray, J. J. (1984). A commentary on Gauss's mathematical diary, 1796–1814, with an English translation. *Expositiones Mathematicae 2*, 97–130.

Johnsen, K. (1984). Zum Beweis von C. F. Gauss für die Irreduzibilität des $p$-ten Kreisteilungspylonoms. *Historia Mathematica 11*, 131–141.

Schneider, I. (1981). Herausragende Einzelleistungen im Zusammenhang mit der Kreisteilungsgleichung, dem Fundamentalsatz der Algebra und der Reihenkonvergenz. In I. Schneider (Ed.), *Carl Friedrich Gauß (1777–1855). Sammelband von Beiträgen zum 200. Geburtstag von C. F. Gauß*, Wissenschaftsgeschichte. Beiträge aus dem Forchungsinstitut des Deutschen Museums für die Geschichte der Naturwissenschaften und der Technik, pp. 37–63. München: Minerva Publikation.

Sørensen, H. K. (1999, November). Niels Henrik Abel and the theory of equations. Appendix of progress report, Institut for Videnskabshistorie, Aarhus Universitet, Aarhus.

Wussing, H. (1969). *Die Genesis des abstrakten Gruppenbegriffes. Ein Beitrag zur Entstehungsgeschichte der abstrakten Gruppentheorie*. Berlin: VEB Deutscher Verlag der Wissenschaften.