Gauss, The Prince of Mathematicians

DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, JUN.

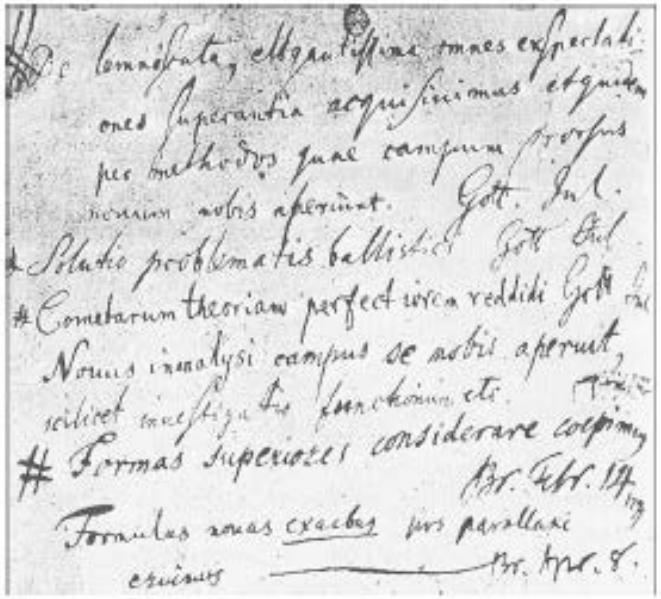
1801.

The Prince of Mathematics

- Carl Friedrich Gauss (1777-1855) is considered the prince of mathematics for several reasons.
- He was a child prodigy. One anecdote relates how the teacher in his kindergarten class asked all the students to add up all the numbers from 1 to 100 in order to keep them quiet. Gauss immediately announced that the sum was 5,050.
- How did he do it? Gauss told the teacher that if you place $1 + 2 + 3 + \ldots + 100$ in the reverse order like $100 + 99 + 98 + \ldots + 1$, the sum in each "column" is 101 and there are a 100 of them.
- Therefore half of this product $(101)(100)$ is the required sum.
- Clearly, Gauss discovered the now well-known formula that $1+2+3+ \ldots + n = n(n+1)/2$ and his method also provides a proof.

The regular 17-gon

- At the age of 19, Gauss solved a major unsolved problem: the construction of the regular 17-gon.
- The ancient Greeks knew how to construct regular n-gons with straightedge and compass for n=3, 5 but no other with a prime number of sides.
- For example, can we construct with straight edge and compass a regular 7-gon? The answer is no, but this was shown much later.
- Gauss was so happy with his discovery that he began a diary. At right, we have a page from his diary.



Facsimile of a page in the famous diary of Gauss

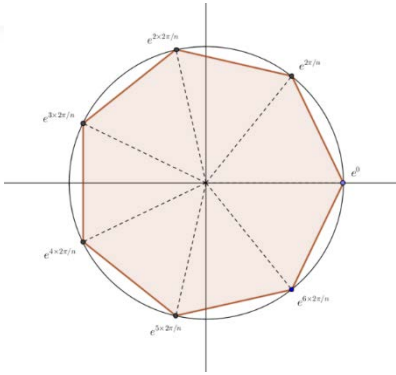
Constructible numbers

- In our earlier lectures, we have already met the idea of constructible real numbers. These are lengths that can be constructed using straightedge and compass.
- But now, we want to enlarge this concept to the realm of complex numbers.

We say a complex number $z = x + iy$ with $x, y \in \mathbb{R}$ is <u>constructible</u> $\Leftrightarrow$ x and y are constructible.

Gauss noticed that the vertices of a regular n-gon can be identified with the n-th roots of unity.

Thus, the problem of constructing a regular n-gon with straight-edge and compass is equivalent to showing all n-th roots of unity are constructible.



Formula for the n-th roots of unity

- We can use de Moivre's formula for writing down the n-th roots of unity.

Recall Euler's theorem $e^{2\pi i} = 1$.

By de-Moivre's theorem

$$e^{2\pi i/n} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

and as $\left(e^{2\pi i/n}\right)^n = 1$ we see that if $z_1 = e^{2\pi i/n}$ then $z_1^n = 1$.

In other words, z_1 is a root of $z^n = 1$.

Notice that if $z_k = z_1^k$ then $z_k^n = 1$ also.

In other words $z_1, z_2, \ldots, z_n$ are roots of $z^n = 1$.

Moreover, these are all distinct. (Exercise)

The field of constructible numbers

The question of constructing a regular n-gon is then reduced to constructing $\mathbb{Z}_1$.

- In an earlier lecture, we saw that if a and b are constructible, then so are ab and a+b. This can be extended to complex numbers also. (Exercise)

The set of all constructible numbers forms a subfield of $\mathbb{C}$. Recall that a field F is a triple $(F, +, \times)$ with two operations denoted + and × and that F is closed under these operations. More precisely $(F, +)$ is an additive group and $(F^\times, \times)$ is a multiplicative group where $F^\times = F - \{0\}$. In addition, we have the distributive laws: $a \times (b+c) = a \times b + a \times c$ and the commutative laws: $a+b = b+a$ and $a \times b = b \times a$.

What does the field of constructible numbers look like?

In an earlier lecture, we proved that if a is constructible, so is $\sqrt{a}$.

Now we proved this for real numbers but it is not hard to extend it to complex numbers because every complex number z can be written as $z = re^{i\theta}$ so if z is constructible, then r is constructible so that $\sqrt{r}$ is constructible.

To construct $\sqrt{z} = \sqrt{r}\, e^{i\theta/2}$ we need to bisect the angle θ which we can do using Euclidean geometry.

- In other words, the only genuinely new constructible numbers we can create from old ones satisfy a quadratic equation. We can make this observation more formal.

The subfield of constructible numbers

- Our discussion shows that the set of all constructible numbers is a subfield of the field of complex numbers. But we can be a bit more precise.

If L and F are fields such that $F \subseteq L$ then we can view L as a vector space over F. If L is a finite dimensional vector space over F we say L has finite degree over F and denote $[L:F]$ as the dimension of L over F.

All of this discussion makes plausible the following theorem:

Main theorem about constructible numbers

Theorem. If $z \in \mathbb{C}$ is constructible, then there is a tower of fields

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_t$$

where $z \in K_t$ and $[K_{j+1} : K_j] = 2 \quad \forall j < t$.

The converse is also true. That is, if z lies in a subfield of $\mathbb{C}$ attainable via quadratic extensions, then z is constructible.

- This theorem turns the geometric problem of constructibility into an algebraic problem about subfields of the complex numbers.

Constructing the regular p-gon for p prime

- Since the problem of constructing the regular p-gon is now the problem of constructing the p-th roots of unity, the previous theorem asks us to determine what is the smallest subfield of **C** in which the p-th roots of unity lie in and if this subfield can be obtained from **Q** in the way described.

Having understood constructibility in this way, we now proceed to determine for which primes p does the number $e^{2\pi i/p}$ lie in such a subfield of $\mathbb{C}$?

Gauss studied the p-th cyclotomic polynomial

$$\frac{z^p - 1}{z - 1} = z^{p-1} + z^{p-2} + \cdots + z + 1$$

Notice this polynomial has degree $p-1$ and has roots

$$z_1 = e^{2\pi i/p}, \quad z_1^2, \quad \ldots, \quad z_1^{p-1}.$$

Eisenstein's criterion for irreducibility

- Gauss showed that this polynomial is irreducible over the rational numbers. A simpler proof was later given by Eisenstein and we adopt his method here.

In other words, we cannot factor

$$z^{p-1} + z^{p-2} + \cdots + z + 1 = f(z)\,g(z)$$

where $f(z)$ and $g(z)$ are polynomials with integer coefficient and of degree smaller than $p-1$.

Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$.
If there is a prime p such that $p \mid a_i$ for all $i < n$ and $p \nmid a_n$, $p^2 \nmid a_0$ then

$f(x)$ is irreducible.

We leave this as an exercise.

Application of Eisenstein criterion to prove irreducibility of the p-th cyclotomic polynomial

We apply the theorem to show that

$$\Phi_p(x) = \frac{x^p - 1}{x - 1}$$

is irreducible if p is a prime number.

Proof. $\Phi_p(x)$ is irreducible $\Leftrightarrow$ $\Phi_p(x+1)$ is irreducible.

Now $$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x}$$

- We can apply the binomial theorem to expand the numerator and simplify/

Applying the binomial theorem

$$(x+1)^p = x^p + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{p-1}x + 1$$

so that

$$\Phi_p(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-2}x + \binom{p}{p-1}$$

Observe that all the coefficients

$$\binom{p}{p-1}, \binom{p}{p-2}, \ldots, \binom{p}{1}$$

are divisible by p. Moreover, $p^2 \nmid \binom{p}{p-1}$ since $\binom{p}{p-1} = p$. The Eisenstein theorem applies and $\Phi_p(x)$ is irreducible.

Gauss theorem on constructing p-gons

- We can now prove Gauss's theorem.

First, what is the smallest subfield of $\mathbb{C}$ that $e^{2\pi i/p}$ lies in over $\mathbb{Q}$?

After some reflection, this turns out to be the field

$$a_0 + a_1 z_1 + \cdots + a_{p-1} z_1^{p-1} \qquad a_i \in \mathbb{Q}$$

and the irreducibility of the cyclotomic polynomial proved above shows that its degree it is $p-1$.

In other words, it is necessary that $p-1$ is a power of 2, say 2^k.

Fermat primes and constructibility

By an exercise in an earlier assignment,

$$p = 2^k + 1 \implies k = 2^n.$$

That is, p must be a Fermat prime.

Now $17 = 2^4 + 1$ is a Fermat prime.

We also see that our field can be obtained via a sequence of quadratic extensions: recall that

$$\cos 2\theta = 2\cos^2\theta - 1$$

$$\implies \cos\theta = \sqrt{\frac{1+\cos 2\theta}{2}}$$

so that each of the numbers

$$e^{2\pi i/4},\ e^{2\pi i/8},\ e^{2\pi i/16},\ \ldots \text{ is constructible.}$$

Duplication of the cube

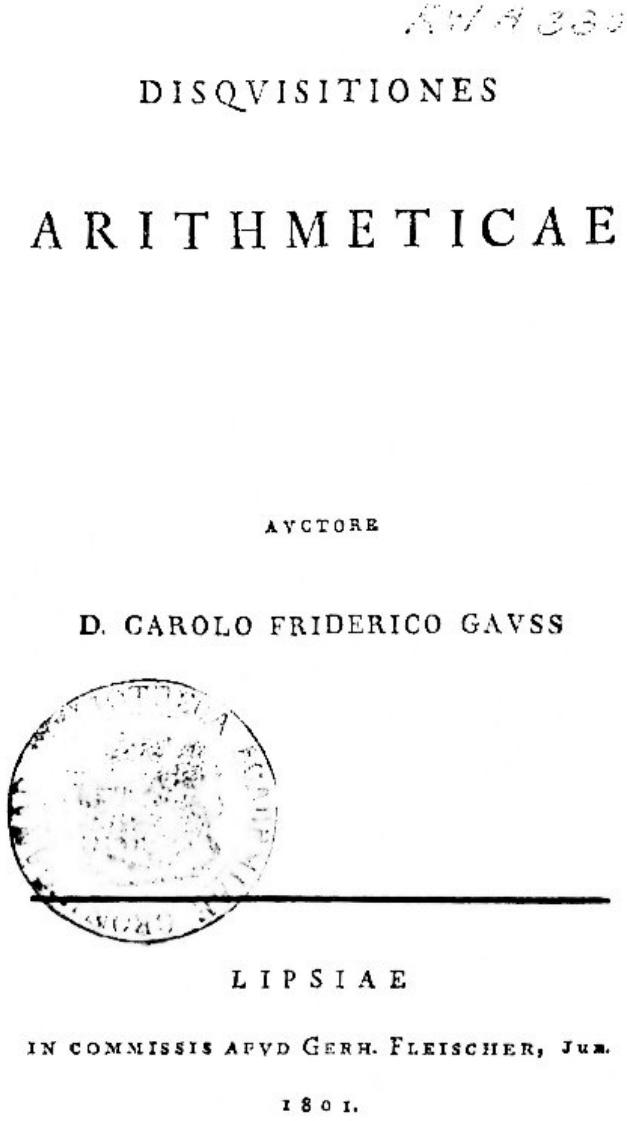
- Since we now have all the tools and theorems at hand, we can dispense with two classical problems immediately, though it was not Gauss who noticed this but rather P.L. Wantzel (1814-1848) in 1837.
- We proved in an earlier lecture that the problem of duplicating a cube is equivalent to constructing the cube root of 2.
- But this number is a root of the polynomial $x^3 - 2$.
- By Eisenstein's criterion applied with p=2, we see the polynomial is irreducible and so, $2^{1/3}$ lies in a field whose degree is 3 over **Q.**
- Since 3 is not a power of 2, the number $2^{1/3}$ is not constructible.
- Observe that this problem was easy to solve once the concepts were in place.

Trisecting a given angle

- We can also show that in general, a given angle cannot be trisected using straightedge and compass by using the same set of ideas.
- Wantzel showed that 60 degrees cannot be trisected using straightedge and compass. The proof is by contradiction.
- If it can, then looking at the angle on a unit circle means that we can construct cos 20^o.
- But cos 3a = $4(\cos a)^3 - 3\cos a$ (exercise) so if $a=20^o$ we see that $z=\cos 20$ is a root of $4x^3 - 3x - ½$ because cos 60=1/2.
- Thus, cos 20 is a root of $f(x) = 8x^3 - 6x - 1$. We want to show this polynomial is irreducible.
- We can apply the same trick as before and consider $f(x-1) = 8x^3 - 24x^2 + 18x - 3$ and apply Eisenstein criterion with p=3 to deduce irreducibility.
- Thus, cos 20 lives in a field of degree 3 over **Q.**
- Hence cos 20 is not constructible.

Disquisitiones Arithmeticae

- Shortly after his PhD, Gauss wrote his famous work, Disquisitiones Arithmeticae in 1801.
- In this work, Gauss introduced the concept of congruences and proved many fundamental theorems that have come to play a major role in the development of mathematics.
- The most notable theorem is the law of quadratic reciprocity, conjectured earlier by Euler and Legendre, who both gave faulty proofs.
- Recall that this theorem relates how the Legendre symbols (p/q) and (q/p) are related.
- More precisely, if p and q are odd primes, then $(p/q)(q/p)=(-1)^{(p-1)(q-1)/4}$.
- Another important contribution is the unique factorization theorem of natural numbers, often attributed erroneously to Euclid.


DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, JUN.

1801.

The distribution of prime numbers

- Gauss also made an important contribution by making a precise conjecture about the distribution of prime numbers.
- This conjecture predicts that the number of primes less than x, often denoted $\pi(x)$ is asymptotic to $x/\log x$.
- This is very close to Legendre's conjecture but not exactly.
- Recall that Legendre conjectured that $\pi(x)$ is asymptotic to $x/(\log x - 1.08366)$.

Gauss's conjecture and Legendre's conjecture compared

Gauss actually made a more precise conjecture that $\pi(x)$ is asymptotic to $\int_2^x \frac{dt}{\log t}$

- This conjecture has now been proved and it disproves Legendre's conjecture.
- To see this, we see from Legendre that $\pi(x)$ is asymptotic to $x/\log x + 1.08366\, x/\log^2 x + O(x/\log^3 x)$.
- But Gauss's conjecture (now a theorem) shows upon integrating by parts that $\pi(x)$ is asymptotic to $x/\log x + x/\log^2 x + O(x/\log^3 x)$.
- We leave the integration by parts as an exercise.
- It is now clear that the 1.08366 is an error and in fact any number there would be an error (Exercise!).
- Gauss's conjecture about $\pi(x)$ was proved in 1896 by Hadamard and de la Vallee Poussin, nearly two centuries after it was stated. We will discuss this in later lectures.