The Practice of Mathematics

Robert P. Langlands

Ars longa, vita brevis

Contents

Lecture series announcement

LECTURE SERIES at the INSTITUTE FOR ADVANCED STUDY

Robert P. Langlands

The Practice of Mathematics

Ars longa, vita brevis

There are several central mathematical problems, or complexes of problems, that every mathematician who is eager to acquire some broad competence in the subject would like to understand, even if he has no ambition to attack them all. That would be out of the question! Those with the most intellectual and aesthetic appeal to me are in number theory, classical applied mathematics and mathematical physics. In spite of forty years as a mathematician, I have difficulty describing these problems, even to myself, in a simple, cogent and concise manner that makes it clear what is wanted and why. As a possible, but only partial, remedy I thought I might undertake to explain them to a lay audience.

I shall try for a light touch including, in particular, some historical background. Nevertheless the lectures are to be about mathematics. In the first set, there will be geometrical constructions, simple algebraic equations, prime numbers, and perhaps an occasional integral. Every attempt will be made to explain the necessary notions clearly and simply, taking very little for granted except the good will of the audience.

Starting in the easiest place for me, I shall give, during the academic year 1999/2000 about eight lectures on pure mathematics and number theory with the motto *beautiful lofty things*. Beginning with the Pythagorean theorem and the geometric construction of the Pythagorean pentagram, I shall discuss the algebraic analysis of geometric constructions and especially the proof by Gauss in 1796 of the possibility of constructing with ruler and compass the regular heptadecagon. This was a very great intellectual achievement of modern mathematics that can, I believe, be understood by anyone without a great aversion to high-school algebra. Then I will pass on to Galois's notions of mathematical structure, Kummer's ideal numbers, and perhaps even the relations between ideal numbers and the zeta-function of Riemann. This material will be a little more difficult, but I see no reason that it cannot be communicated. It brings us to the very threshold of current research.

Since this attempt is an experiment, the structure and nature of the lectures will depend on the response of the audience and on my success in revealing the fabric of mathematics. If it works out, I would like to continue in following years on classical fluid mechanics and turbulence, with motto *l'eau mêlée à la lumière*, and then, with the somewhat trite motto с того берега, on the analytical problems suggested by renormalization in statistical mechanics and quantum field theory.

West Building Lecture Hall, Institute for Advanced Study
Tuesdays at 4:30pm
October 26, November 2, 9, 16 and February 1, 8, 15, 22

On the use of these notes

The texts and diagrams collected below can be read independently or used as supplements to the video-tapes of the lectures. They include not only copies of the transparencies used during the course of the lectures, but also copies of various texts cited, together with translations, as well as the lecturer's own preparatory notes.

There was no clean division of the lectures into eight, or if the whole year is taken into account sixteen, hours, so that it would be futile to divide these notes into separate sections. The lectures overlapped, the end of one running into the beginning of the next, and transparencies were sometimes displayed more than once. None the less, for the convenience of the viewer, for each lecture a precise location is indicated at which he can conveniently begin to read or to peruse the material pertinent to it.

The lyf so short, the craft so long to lerne,
Th'assay so hard, so sharp the conquering.

Lecture 1

The decision to deliver these lectures arose from two sources. First of all, the Faculty of the Institute is being encouraged by our employers to leave, at least for brief moments, the confines of our disciplines and to present ourselves to the public at large. This is, in my view, an excellent idea, but the format chosen, one-hour public lectures, is not congenial to all of us, certainly not to me. It is never clear what to present. In particular, my own elucubrations lead at best infrequently to something that is worth communicating even to specialists, and even then they are not easily persuaded, if at all. So I hesitate to impose any discovery of mine on an innocent public.

On the other hand, I, like many other mathematicians, have spent, even perhaps wasted, much time on a large variety of problems on which I could make no inroads, so that my efforts have left no trace. Now, it is seldom the habit of mathematicians when they attack a problem to study systematically its history or the literature surrounding it, at least this has not been my habit. The youthful impulse is rather to prowl about the problem for a while, looking perhaps not for an open window or a door with a weak lock, for if these were available, some earlier malefactor would already have discovered them, but for some wall that can be scaled or some unsuspected underground access. The upshot is that if nothing is discovered, one comes away from the effort empty-handed, having learned little, except what to avoid.

With waxing age and waning energies a different impulse manifests itself, not the desire to overwhelm this or that outstanding problem by force or cunning but rather the desire to understand its sources and to formulate clearly its meaning and significance. Nevertheless, without some external compulsion or, at least, encouragement, this impulse would in all likelihood come to naught for what a mathematician, even an elderly one, really wants to do is discover new theories, new techniques and new methods and to solve the old problems. In an attempt to exploit to my own profit my new obligation to come out of the closet, and to kill two birds with one stone, I announced these lectures, from which I hope both you and I will be able to learn some genuine mathematics. I have already learnt a good deal that I did not know before. In preparing the lectures I have kept in mind especially those among my colleagues in the humanities who have frequently assured me of their desire to acquire some understanding of the subject. I am not sure how sincere they are, but I count on them, and on all of you, to let me know if my instructional efforts are failing and not simply by failing to mention.

Indeed, there are many reefs on which this undertaking can run aground. My inexperience with much of the material may turn out to be an advantage, but my

---

Date of lecture: Fall term, October 26, 1999.

pedagogical inadequacies are a handicap. Moreover, although these lectures are aimed at an audience whose experience with mathematics may have ended with high school the bulk of you are undoubtedly professional mathematicians whose expectations may or may not be deceived. A number of the mathematicians, like me, will have been educated in inadequate North American schools and may, therefore, have had little experience with classical introductory mathematics, so the beginnings may amuse them. Even so, the moral pressure on me to move at too fast a pace will be great, and I am not entirely confident of my courage to resist it. Questions and observations that slow me down will be much appreciated.

Although the plans as announced are on the whole are rather grandiose, I still have only the vaguest ideas what I will do in the series on fluid mechanics or on statistical mechanics and renormalization promised for subsequent years. I thought it would be best to let the future take care of itself. I am already uneasy enough about the second term's set of lectures. For the first term, the plans are fairly clear, although the timing is uncertain. Four weeks may not be enough and I may have to run over.

FALL TERM

(I) Introductory geometrical material—the Pythagorean theorem.
(II) Geometrical construction of regular pentagon.
(III) Analytic geometry and complex numbers.
(IV) Gauss's construction of the regular heptadecagon.

TWO MAJOR WORKS

Euclid's Elements and Gauss's Arithmetical Investigations

Comment on plan

It may be useful to explain briefly the structure of this set of lectures. The purpose of the Pythagorean theorem in the context of the construction of the regular pentagon is to construct a certain quadratic irrational or surd, a notion to be explained. The first impression of some may be that this is simply a rehash of high-school geometry, but quadratic irrationals remain of major interest even today and the nature of other irrationals (icosahedral for example) is a central problem. They were, as will be observed in passing, the source of a crisis in Greek mathematics that lasted more than a century and that was only resolved by a new understanding of the notion of number. If I were better informed I would spend more time discussing this crisis and its resolution.

The regular pentagon has, as I shall recall, an evident five-fold geometric symmetry. It also has, although this is far from evident, a four-fold symmetry that is the clue to its geometric construction, but of which the Greeks were unaware. This symmetry is revealed by an algebraic analysis that can only be carried out with the help of complex numbers, so that some time has to be spent introducing them to you and explaining their role in analytic geometry. Complex numbers are second nature to those with any mathematical training, but not to others. Since it is the others to whom these lectures are addressed, I shall spend the necessary time on them.

The hidden four-fold symmetry of the pentagon understood, we shall be in a position to understand the hidden sixteen-fold symmetry of the regular seventeen-sided polygon that permits it to be constructed geometrically. In contrast the heptagon, with seven sides and a hidden six-fold symmetry cannot be constructed geometrically, that is—to be more explicit about what is here intended by the adverb *geometrically*—with the aid of nothing but a ruler and a compass. The difference between 5, 7 and 17 is that

$$4 = 2 \cdot 2, \quad 16 = 2 \cdot 2 \cdot 2 \cdot 2 \quad \text{but} \quad 6 = 2 \cdot 3.$$

We want to understand why this difference in the factorization of the three numbers has such a striking geometric consequence.

That it did was discovered by Gauss as a lad of 18 in 1796. This is often presented as a curious juvenile achievement of little import in comparison with his other early achievements, accomplished when he was scarcely older. It would be better if I were able to say, when the time comes, more about Gauss. I fear that in the past I instinctively avoided acknowledging what it meant to be a real mathematician. So I cannot now give you any information beyond the familiar. He was extremely precocious, extremely powerful and inventive, with an apparently innate mathematical curiosity that I now appreciate is rare. Mathematical talent is perhaps more common than mathematical curiosity. Although born to parents of little or no means, his gifts were noticed early, and he was educated at the expense of the Duke of Brunswick, presumably with the expectation that he would become a functionary of some sort. Although the talents encouraged were apparently linguistic and not mathematical he found himself at schools with good mathematics libraries and seems to have made himself familiar with some of the important mathematical research of the eighteenth century, including that of Euler and Lagrange, not only mastering it but also deepening it.

The construction of the regular heptadecagon could appear, if so presented, as a spontaneous contribution of an adolescent, but seems rather to have been rendered possible by Gauss's facility with the complex numbers developed in the course of the century and by his familiarity with Lagrange's attempts to analyze the solution of equations by radicals. What may have been spontaneous in his achievement was the return after more than two millennia to an ancient geometric problem, the construction of regular polygons, that had been abandoned because of the difficulties appearing for heptagons. But I do not know. Here, as elsewhere in the preparation of these lectures, I am brought face to face with my ignorance.

The plan and its structure are now clear, as is one glaring defect. One hour for the material in each of the four sections is not enough. An hour is not enough to make the material comprehensible and it is not enough to make the presentation fun. Once started, for example, on the construction of the pentagon, I found the geometry irresistible.

My feeling for the Greeks as mathematicians is every bit as inadequate as that for the youthful Gauss. I do not know whence came their curiosity and depth. Perhaps no one does. We live in a highly structured environment dedicated to research. We earn our living by it and we pin our hopes of recognition on it, but the questions we ask and the problems we solve are determined more by tradition, more by our colleagues than by our own natural and spontaneous curiosity. We are seldom playful; our efforts are never simply for our own amusement. A brief romp with Greek mathematics in which we examine the construction of the pentagon at length may be an occasion to capture briefly the ludible spirit of the Greeks.

An hour is also not enough for an adequate understanding of analytic geometric and complex numbers nor for a presentation of the algebra required for Gauss's construction. The complex numbers are an enormously effective tool that swallows the geometry, but it will be good to ask ourselves how. Moreover the four-fold or sixteen-fold algebraic symmetry is far more subtle than the five-fold or seventeen-fold geometric symmetry. Since it will reappear again and in spades when, and if, we discuss Galois and Kummer, it is best to get used to it now.

The upshot is that four hours is scarcely enough. My plan is, therefore, simply to go on, probably for another four weeks, so that I will not have finished this first set until sometime in December. All being well, this will leave me some listeners and enough time to prepare for the second set in February.

$$5 - 1 = 4 = 2 \times 2$$

$$17 - 1 = 16 = 2 \times 2 \times 2 \times 2$$

BUT

$$7 - 1 = 6 = 2 \times 3$$

Rainer Maria Rilke
Der Schauende

Ich sehe den Bäumen die Stürme an,
die aus laugewordenen Tagen
an meine ängstlichen Fenster schlagen,
und höre die Fernen Dinge sagen,
die ich nicht ohne Freund ertragen,
nicht ohne Schwester lieben kann.

Dageht der Sturm, ein Umgestalter,
geht durch den Wald und durch die Zeit,
und alles ist wie ohne Alter:
die Landschaft, wie ein Vers im Psalter,
ist Ernst und Wucht und Ewigkeit.

Wie ist das klein, womit wir ringen,
was mit uns ringt, wie ist das groß;
Ließen wir, ähnlicher den Dingen,
uns so vom großen Sturm bezwingen –
wir würden weit und namenlos.

Was wir besiegen, ist das Kleine,
und der Erfolg selbst macht uns klein.
Das Ewige und Ungemeine
will nicht von uns gebogen sein.
Das ist der Engel, der den Ringern
des Alten Testaments erschien;
wenn seiner Wildersacher Sehnen
im Kampfe sich metallen dehnen,
fühlt er sie unter seinen Fingern
wie Saiten tiefer Melodien.

Wen dieser Engel überwand,
welcher so oft auf Kampf verzichtet,
der geht gerecht und aufgerichtet
und groß aus jener harten Hand,
die sich, wie formend, an ihn schmiegte.
Die Siege laden ihn nicht ein.
Sein Wachstum ist: Der Tiefbesiegte
von immer Größerem zu sein.

Созерцание

Деревья складками коры
Мне говорят об ураганах,
И я их сообщений странных
Не в силах слышать средь нежданных
Невзгод, в скитаньях постоянных,
Один, без друга и сестры.
Сквозь рощу рвется непогода,
Сквозь изгороди и дома.
И вновь без возраста природа,
И дни, и вещи обихода,
И даль пространств — как стих псалма.
Как мелки с жизнью наши споры,
Как крупно то, что против нас!
Когда б мы поддались напору
Стихии, ищущей простора,
Мы выросли бы во сто раз.
Все, что мы побеждаем, — малость,
Нас унижает наш успех.
Необычайность, небывалость
Зовет борцов совсем не тех.
Так ангел Ветхого завета
Нашел соперника под стать.
Как арфу, он сжимал атлета,
Которого любая жила
Струною ангелу служила,
Чтоб схваткой гимн на нем сыграть.
Кого тот ангел победил,
Тот правым, не гордясь собою,
Выходит из такого боя
В сознаньи и расцвете сил.
Не станет он искать побед.
Он ждет, чтоб высшее начало
Его все чаще побеждало,
Чтобы расти ему в ответ.

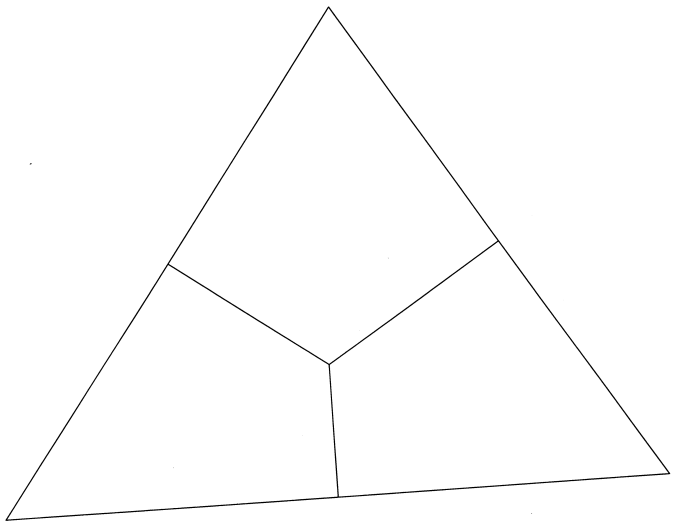
Habe Furcht vor dem großen Sturm,
und gib acht auf den kleinen Wind.

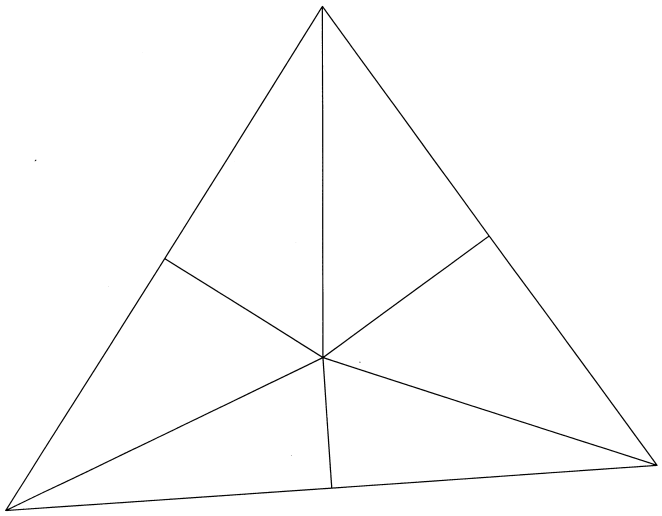
Transitional remarks

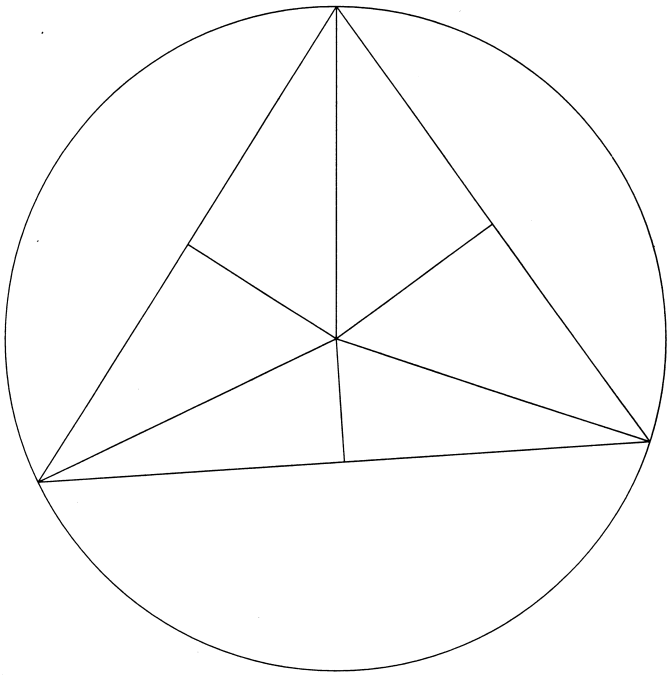
As a start, I return just for a minute to the beginnings of my unsuccessful effort over more than four decades to master a difficult trade. Through a kind of fluke I found myself at university at quite an early age—not quite seventeen—but with no preparation, whereupon on an impulse that I think I now understand I decided, with no notion whatsoever of mathematics or physics and no notion whatsoever of academic life, that I wanted to be a mathematician or perhaps a physicist. Although physics turned out finally to be too difficult for me, I did come across not long after this decision a copy of the Einstein volume in Schilpp's series of hefty tomes *The Library of Living Philosophers*. It was in the windows of a stationer's shop in the town near to the hamlet in which I grew up. (For those who are familiar with the local topography, it was on the corner of Columbia Ave. and 6th St. in New Westminster.)

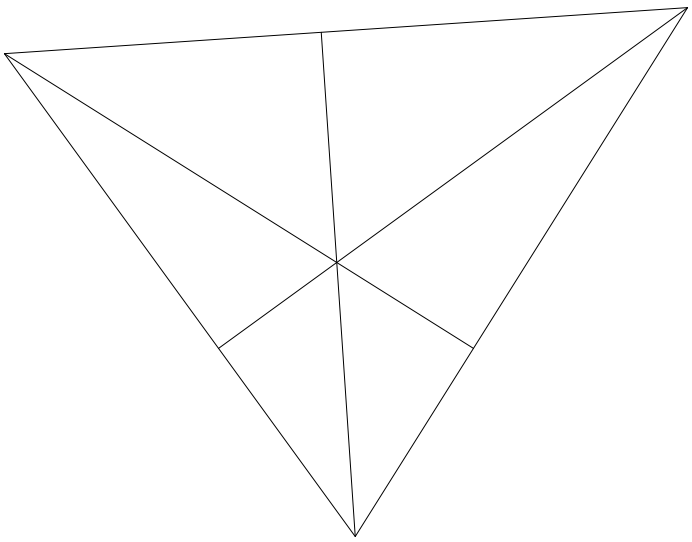
I still have it although I never made much of it, but there was a brief intellectual biography by Einstein in which he describes two memorable intellectual experiences of his childhood: his introduction to a compass at the age of five and his discovery of Euclid at the age of twelve. Although an uncle appears to have introduced him to euclidean geometry and the Pythagorean theorem even earlier, at that age he was presented with what was then a widely used text *Lehrbuch der Geometrie zum Gebrauch an höheren Lehranstalten* that thanks to our librarian, Momota Ganguli, I was able to have a look at. Although obscure in places, it appears a book rich in content that well deserved its success. Einstein cites explicitly the theorem that especially impressed him, oddly enough a theorem that is not to be found in the Elements, although it was presumably known at the time and to Euclid. It is an elegant fact with an elegant proof and quite simple, so that, as a warm-up, I begin with it.

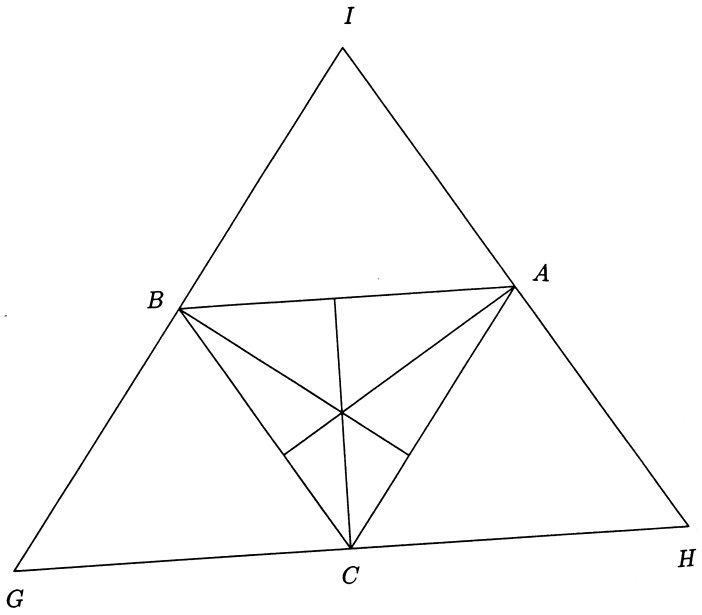
Anyhow, without any background in mathematics myself, and not knowing where to begin, I followed Einstein's implicit recommendation and acquired a copy of the Elements (Todhunter's edition in the Everyman collection, a very popular, very cheap collection of my youth and still, in my view, very useful). I did not make much headway with it. There were several reasons, not least, but not only, my uncertain intellectual taste. I already knew about analytic geometry and it was clear that most, perhaps all, the geometrical propositions of Euclid, which were the ones I was looking at, could be proved much more quickly algebraically. Since I had a lot of time to make up, I very quickly abandoned the geometry as such. In retrospect it is clear that the Elements is a much more complex and sophisticated text, both scientifically and historically, than I was able to deal with at the time.











$$\left.\begin{array}{l} BC = AH \\ BC = AI \end{array}\right\} \Longrightarrow AH = AI$$

Heath's introduction to the Everyman edition

It was with the greatest interest that I heard that the publishers thought of adding to Everyman's Library an edition of the *Elements* of Euclid; for what book in the world could be more suitable for inclusion in the Library than this, the greatest textbook of elementary mathematics that there has ever been or is likely to be, a book which, ever since it was written twenty-two centuries ago, has been read and appealed to as authoritative by mathematicians great and small, from Archimedes and Apollonius of Perga onwards? No textbook, presumably, can ever be without flaw (especially in a subject like geometry, where some first principles, postulates or axioms, have to be assumed without proof, and any number of alternative systems are possible), and flaws there are in Euclid; but it is safe to say that no alternative to the *Elements* has yet been produced which is open to fewer or less serious objections. The only general criticism of it which is deserving of consideration is that it is unsuitable as a textbook for very young boys and girls who are just beginning to learn the first things about geometry. This can be admitted without detracting in the least from the greatness or the permanent value of the book. The simple truth is that it was not written for schoolboys or schoolgirls, but for the grown man who would have the necessary knowledge and judgment to appreciate the highly contentious matters which have to be grappled with in any attempt to set out the essentials of Euclidean geometry as a strictly logical system, and, in particular, the difficulty of making the best selection of unproved postulates or axioms to form the foundation of the subject. My advice would, therefore, be: if you must spoon-feed the very young, do so; but when they have shown a taste for the subject and attained the standard necessary for passing honours examinations, let them *then* be introduced to Euclid in his original form as an antidote to the more or less feeble echoes of him that are to be found in the ordinary school textbooks of 'geometry'. I should be surprised if such qualified readers, making the acquaintance of Euclid for the first time, did not find it fascinating, a book to be read in bed or on a holiday, a book as difficult as any detective story to lay down when once begun. I know of one actual case, that of an undergraduate at Cambridge suddenly presented with a copy of Euclid, where this happened. This is the true test of such a book. Nor does the reading of it require the 'higher mathematics'. Any intelligent person with a fair recollection of school work in elementary geometry would find it (progressing as it does by gradual and nicely contrived steps) easy reading, and should feel a real thrill in following its development, always assuming that enjoyment of the book is not marred by any prospect of having to pass an examination in it! This is why I applaud the addition of this great classic to Everyman's Library; for everybody ought to read it who *can*, that is, all educated persons except the very few who are constitutionally incapable of mathematics.

Euclid and Harish-Chandra

In the early sixties, the mathematician Harish-Chandra joined the Faculty of the Institute, At that time his papers were much admired but little read. They were regarded as too difficult. Their purpose was to be correct, they took no pity on the reader, but moved forward relentlessly, lemma after lemma, theorem after theorem, paper after paper with little attempt to distinguish the real obstacles from the more straightforward development. Euclid, to whom I now come long after reading much of Harish-Chandra, has a similar style, so that I am struck with admiration for any

school-boy of an earlier era who drew his intellectual nourishment directly from Euclid. I recall that Einstein did not.

Lecture 2

Pythagoras 530 BC

Plato 380 BC

Eudoxus 360 BC

Aristotle 340 BC

Euclid 290 BC

Date of lecture: Fall term, November 2, 1999.

It will be clear both from the announcement and the exculpatory remarks that my intention is to clarify both for myself and for the audience some problems of contemporary mathematics, and that any historical preliminaries are principally for the sake of clarifying the mathematical issues, not the historical issues. I want therefore to stress once again that when it comes to mathematics in antiquity or even during the Renaissance, I am almost immediately in over my head. In particular, since I make a few remarks concerning Pythagoras and the Pythagorean theorem that may belong more to the realm of myth than of history, it may be best as a warning to the audience to cite some phrases from the book of Otto Neugebauer, a historian of science who, I recall for the younger members of the audience, spent the last years of his life attached to the Institute.

Some quotations from

O. Neugebauer's
The exact sciences in antiquity

1. The above example of the determination of the diagonal of the square from its side is sufficient proof that the "Pythagorean" theorem was known more than a thousand years before Pythagoras.
2. It seems to me evident, however, that the traditional stories of discoveries made by Thales or Pythagoras must be discarded as totally unhistorical.
3. We know today that all the factual mathematical knowledge which is ascribed to the early Greek philosophers was known many centuries before, though without the accompanying evidence of any formal method which the mathematicians of the fourth century would have called a proof. For us, there is nothing to do but to admit that we have no idea of the role which the traditional heroes of Greek science played.
4. The Greeks themselves had many theories about the origins of mathematics. ... A much more sophisticated attitude is represented by Aristotle, who considers the existence of a "leisure class", to use a modern term, a necessary condition for scientific work. Our factual knowledge about the development of scientific thought and of the social position of the men who were responsible for it is so utterly fragmentary, however, that it seems to me completely impossible to test any such hypothesis, however plausible it may appear to a modern man.

The exact sciences in antiquity: extract

This is confirmed by a small tablet, now in the Yale Babylonian Collection. On it is drawn a square with its two diagonals. The side shows the number 30, the diagonal the numbers 1, 24, 51, 10 and 42, 25, 35. The meaning of these numbers becomes clear if we multiply 1, 24, 51, 10 by 30, an operation which can easily be performed by dividing 1, 24, 51, 10 by 2 because 2 and 30 are reciprocals of each other. The result is 42, 25, 35. Thus we have obtained from $a = 30$ the diagonal 42; 25, 35 by using

$$\sqrt{2} = 1; 24, 51, 10.$$

The accuracy of this approximation can be checked by squaring 1; 24, 51, 10. One finds

$$1; 59, 59, 59, 38, 1, 40$$

corresponding to an error of less than $22/60^4$.

Comments

$$1;24,51,10 \div 2 = 0;30+0;12+0;0,25+0;0,0,30+0;0,0,5$$
$$= 0;42,25,35$$

$$1 + \frac{24}{60} + \frac{51}{60^2} + \frac{10}{60^3} = 1.41421296\ldots$$

$$2 \times 24 = 48; \qquad 2 \times 51 = 1,42; \qquad 2 \times 10 = 20;$$
$$24 \times 24 = 9,36; \qquad 51 \times 51 = 43,21; \qquad 10 \times 10 = 1,40;$$
$$24 \times 51 = 20,24; \qquad 24 \times 10 = 4,0; \qquad 51 \times 10 = 8,30;$$

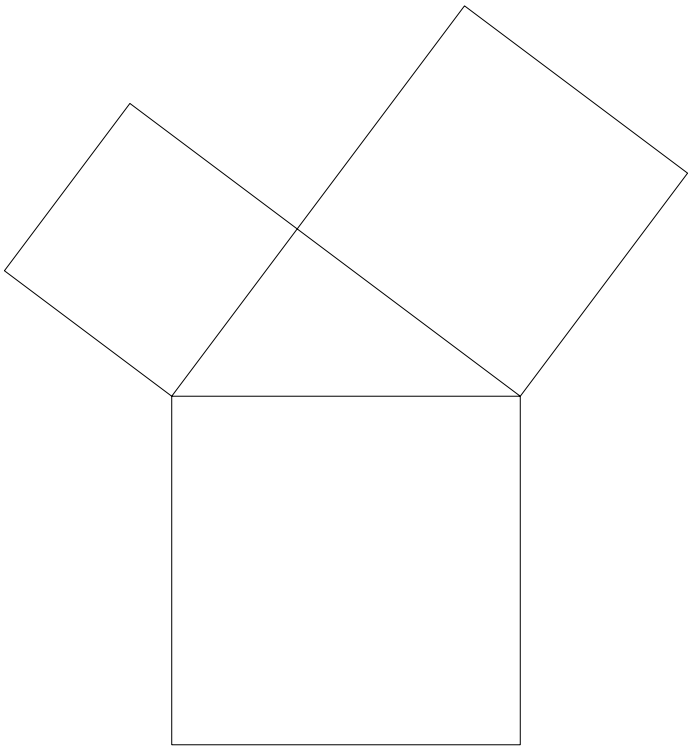
Doubled: 40, 48; 8, 0; 17, 0;

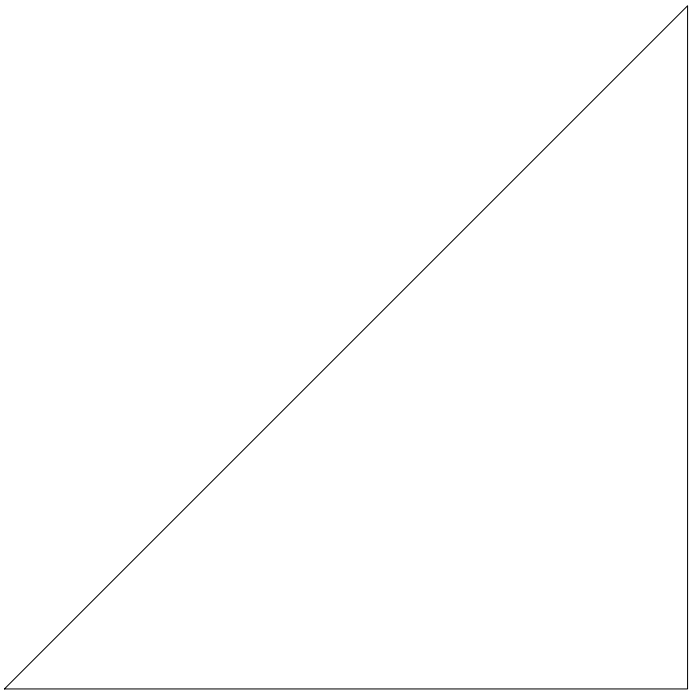
Thus 1; 24, 51, 10 squared is

$$1;+;9,36+;0,0,43,21+;0,0,0,0,1,40+;$$
$$48+;1,42+;0,0,20+;0,40,48+;0,0,8+;0,0,0,17$$

or

$$1;59,59,59,38,1,40$$



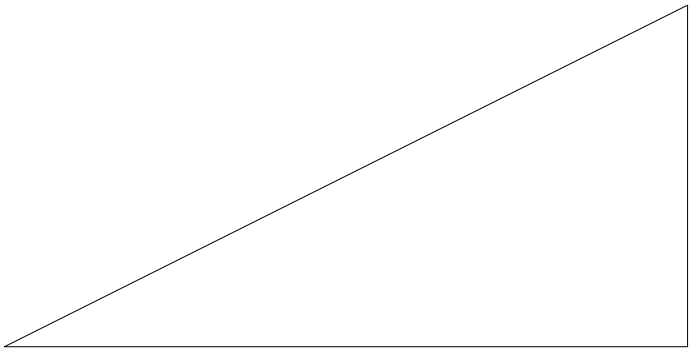


$$2 = \frac{a^2}{b^2}$$

$$2b^2 = a^2$$

$$a = 2c, \quad 2b^2 = 4c^2, \quad b^2 = 2c^2$$

Thus a and b both even.



$$5 = \frac{a^2}{b^2}$$

$$5b^2 = a^2$$

$$a = 5c, \quad 5b^2 = 25c^2, \quad b^2 = 5c^2$$

Thus a and b both divisible by 5.

Aristotle: Analytica Priora

For all who effect an argument *per impossibile* infer syllogistically when something impossible results from the assumption of its contradictory; e.g. that the diagonal of the square is incommensurate with the side, because odd numbers are equal to evens if it is supposed to be commensurate. One infers syllogistically that odd numbers come out equal to evens, and one proves hypothetically the incommensurability of the diagonal, since a falsehood results through contradicting this.

Plato: Theaetetus

SOCRATES: But I am more interested in our own Athenian youth, and I would rather know who among them are likely to do well. Tell me then, if you have met with any who is at all remarkable.

THEODORUS: Yes, Socrates, I have become acquainted with one very remarkable Athenian youth, whom I commend to you as well worthy of your attention. If he had been a beauty I should have been afraid to praise him, ...

SOCRATES: Herein lies the difficulty which I can never solve to my satisfaction—What is knowledge?

THEODORUS: I would rather that you would ask one of the young fellows.

THEAETETUS: Theodorus was writing out for us something about roots, such as the sides of squares three or five feet in area showing that they are incommensurable by the unit: he took the other examples up to seventeen, but there for some reason he stopped. Now as there are innumerable such roots, the notion occurred to us of attempting to find some common description which can be applied to them all.

The comments at the end of the first talk that were not about Rilke were about square roots, and in particular about the proof that $\sqrt{2}$ and $\sqrt{5}$ are irrational. So I want to make a couple of additional remarks.

I give first of all, two standard quotations, one from Aristotle and one from Plato. The one from Aristotle makes clear that the arithmetic proof of the irrationality of $\sqrt{2}$ that I presented was not too much of an anachronism, even if it was not the first proof discovered by the Greeks. This is not certain. There is a second proof, a geometric proof. This can be construed as a proof by paper-folding and was shown to me by one member of the audience. It has been suggested, for various reasons, that the first proof ever given may have been geometric, but there is apparently no solid, universally accepted evidence or argument one way or the other.

Although the dialogue Theaetetus is not primarily concerned with mathematics but with other matters, I cite selectively from it to obtain a dialogue appropriate to our purposes. Theodorus, apparently a celebrated geometer but known largely through this text was the teacher of Theaetetus. That he stopped at 17 has been taken as evidence that his proof must have been difficult of execution, for example geometric, and not along the line of the one I gave for $\sqrt{5}$. Hardy and Wright in their *Introduction to the theory of numbers* are not at all persuaded by this line of argument. In any case the issue with Theodorus is not $\sqrt{2}$ but the square roots of larger numbers, 3, 5 and so on up to 17, with of course 4, 9, and 16 omitted.

Hardy and Wright offer, however, both arithmetic and geometric proofs, and it is worthwhile having a look at their discussion.

I observe in passing that Theodorus seems to have had an anxious administration, fearful of sexual harassment charges, looking over his shoulder.

The importance of the discovery of the irrationality of $\sqrt{2}$ and of the crisis it caused in Greek mathematics is germane to the story I want to relate only in so far as we want to arrive at some understanding of the contemporary problems posed by irrationality, and indeed by irrationality of a special kind, by algebraic irrationality, a notion that it will take us some time to reach. None the less, a few succinct quotations from Neugebauer and from Heath may not be out of place, especially since as was observed to me by a friend, Eudoxus, the great mathematician who resolved the crisis, may be quite unfamiliar to mathematicians. I cannot say that his name had been familiar to me.

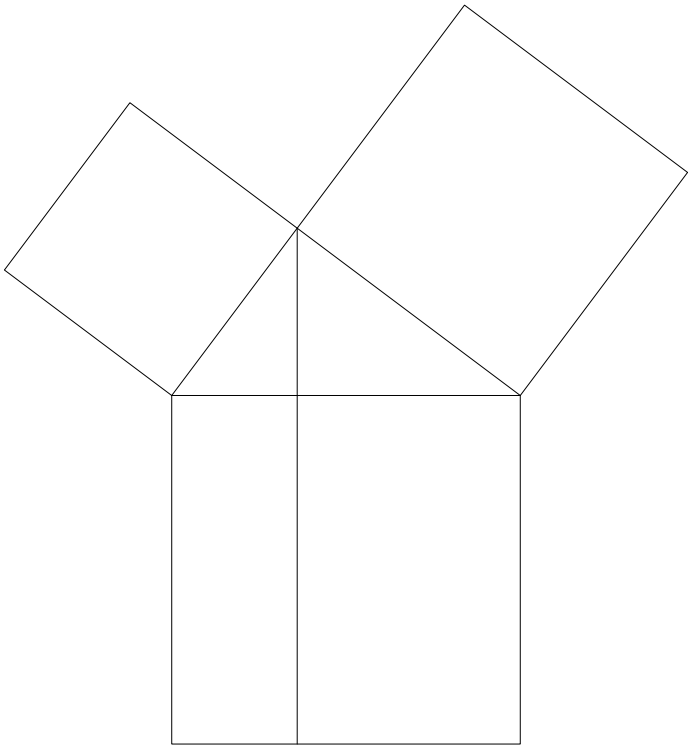
Observe (perhaps!) that one thing that emerges from the comments of Neugebauer is that the geometrical treatment which I follow was the result of the Greek's geometrical treatment of number, somewhat of a historical accident and apparently peculiar to the Greeks, as other mathematicians of antiquity without the Greek's respect for logic proceeded differently. Since the geometrical treatment is, as we shall see, much less straightforward than an algebraic treatment, it may be that the historical approach obscures as much as it enlightens.

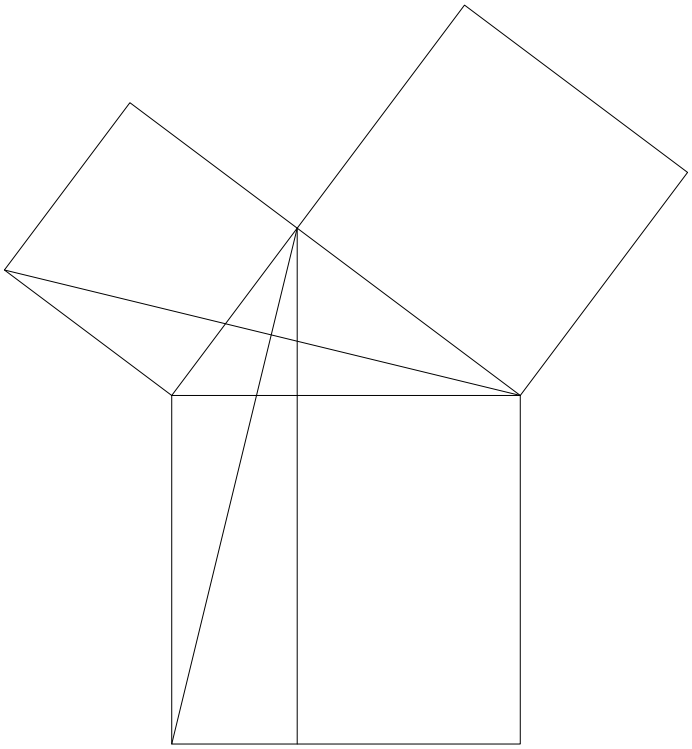
1. (Neugebauer). It is also generally accepted that the essential turn in the development came about through the discussion of the consequences of the arithmetical fact that no ratio of two integers could be found such that its square had the value 2. The geometrical corollary that the diagonal of the square could not be "measured" by its side obviously caused serious discussion about the relation between geometrical and arithmetical proof. ... The reaction of the mathematicians ... led to two major steps. ... this gave rise to the strictly axiomatic procedure. Secondly, it had become clear that one should consider the geometrical objects as the given entities such that the case of integer ratios appeared as a special case of only secondary interest.

2. (Heath). *Theory of proportion.* The anonymous author of a scholium to Euclid's Book V ... tells us ... that this Book, containing the general theory of proportion... 'is the discovery of Eudoxus, the teacher of Plato'. There is no reason to doubt the truth of this statement. ...

The essence of the new theory was that it was applicable to incommensurable as well as commensurable quantities; and its importance cannot be overrated, for it enabled geometry to go forward again, after it had received the blow which paralyzed it for the time. This was the discovery of the irrational, at a time when geometry still depended on the Pythagorean theory of proportion, that is, the numerical theory which was of course applicable only to commensurables. ...

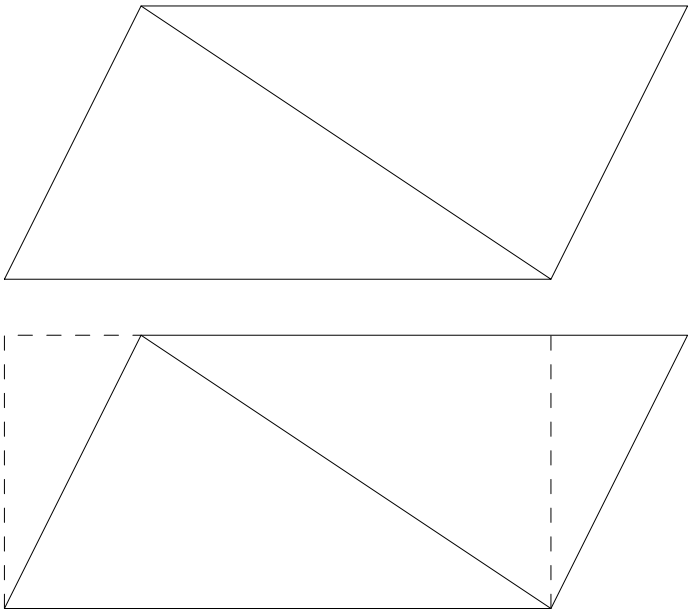
The greatness of the new theory itself needs no further argument when it is remembered that the definition of equal ratios in Eucl. V, Def. 5 corresponds exactly to the modern theory of irrationals due to Dedekind, and that it is word for word the same as Weierstraß's definition of equal numbers.





Area of a triangle

$$\text{Area} = \frac{1}{2} \times \text{Base} \times \text{Height}$$



A difficulty

I introduce the formula for the area of a triangle, as it is familiar, but in the euclidean context an area is an area and a number is a number, and they are different things. We should rather, in Euclid's terms, speak of the area of a parallelogram being double of that of the triangle or simply of the parallelogram being double the triangle, but leave this aside for the moment.

Since a triangle has three different sides, each of which can be taken as the base, and correspondingly three different heights, the formula for the area is in fact three formulas, and one may ask why they should give the same result. In fact, this question is not addressed in Euclid. It appears, as my colleague Pierre Deligne pointed out to me, to be an implicit, not explicit, assumption on the part of Euclid that the area of a plane figure is a well-defined notion and that it is additive, thus if one figure is decomposed into the sum of two, as a parallelogram is decomposed into the sum of two triangles, then the area of the larger will be the sum of the areas of the smaller.

This difficulty vitiates, as Deligne observed, Euclid's proof of the Pythagorean theorem. I run through Euclid's proof and various alternate proofs, and then return to the difficulty.

Hilbert treats the definition of areas of polygons in his book *Grundlagen der Geometrie*, the basic problem being to show that the area is well-defined. He begins by showing that the three possible formulas for the area of a triangle all give the same result. For this he needs the theory of similar triangles, thus the theory of proportions or Book V of Euclid. In other words, from an even more rigorous point of view Euclid's efforts to avoid this theory in his early chapters have been in vain. Areas can only be adequately defined by introducing numbers, thus proportions, and by establishing some consequences of the theory of proportions, thus the theory of similar triangles.

Eudoxus and Grothendieck

Euclid's proof of the Pythagorean theorem has been a puzzle to many people. Nietzsche apparently found it *stelzbeinig* and *hinterlistig*, thus stilted and sly, and he was not far off the mark. Aldous Huxley, in a short story about thwarted mathematical genius *Young Archimedes* suggests, and he has the support of some historians of mathematics, that Pythagoras was likely to have used a simpler, more geometrically evident proof.

First alternate proof. It seems, however, that in spite of the appeal of this proof most historians are of the opinion that it does not have a Greek feel. Heath presents a proof that is possibly Greek, and possibly the one used by Pythagoras or his school.

Second alternate proof. The difficulty is that it uses the notion of similar triangles, and similar triangles are first discussed by Euclid in Book VI after he has developed, following Eudoxus, the theory of proportions in Book V. The theory of proportions is, if one likes, the theory of pure numbers, as opposed to lengths or areas, a notion whose difficulty appears when it is recognized that not all lengths or areas are multiples of one aliquot part, as the Greeks discovered as a consequence of the Pythagorean theorem, so that there are pure numbers that are not representable as fractions a/b. Thus, it appears that the first proof of the Pythagorean theorem was by a method which was revealed by further deductions from the theorem as flawed.

One aspect of the art of mathematics is the formulation of good definitions. In the second half of the twentieth century Grothendieck was the master of this. His definitions, with a breathtaking clarity, often transformed what had previously been regarded as an arcane, difficult theory, for example, that of complex multiplication, into self-evident consequences. A first reading of Euclid on proportions suggests that Eudoxus may have been the Greek Grothendieck. The proof of Proposition VI.1, accessible to all of you, is an elegant example of what can be done with a good definition. I recommend it as supplementary reading.

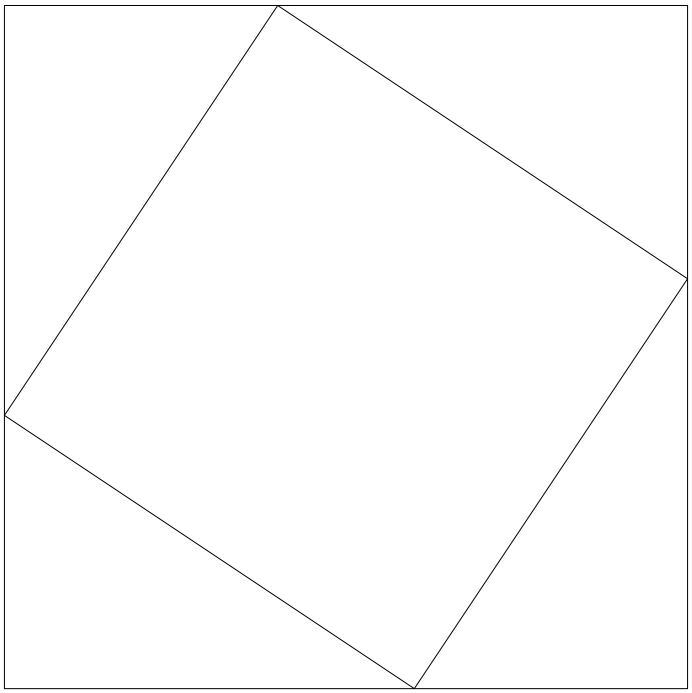
Proposition VI.1. *Triangles and parallelograms which are under the same height are to one another as their bases.*

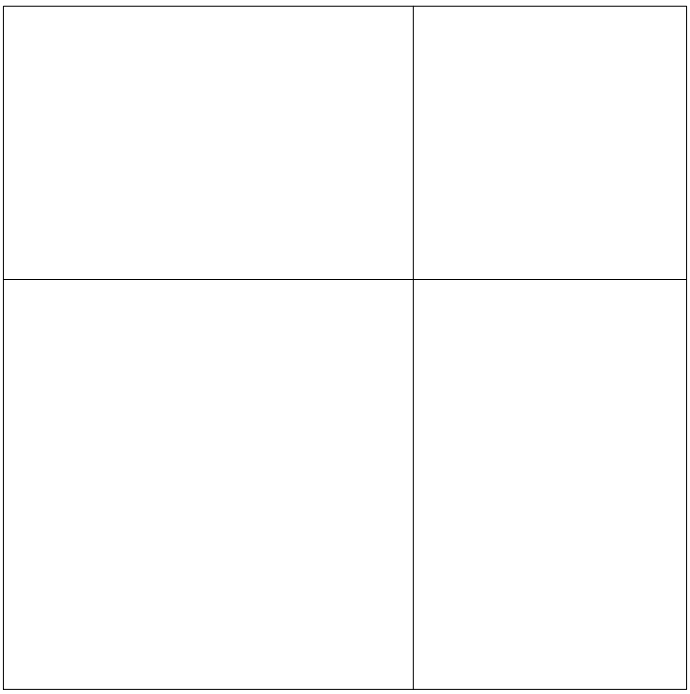
At all events, Euclid's proof of Proposition I.47, the Pythagorean theorem, appears, as Heath argues, to be Euclid's original response to an expository challenge. He needed the theorem early; yet he was not permitted to use the earlier proof because he had not yet developed the theory of proportions and the theory of similar

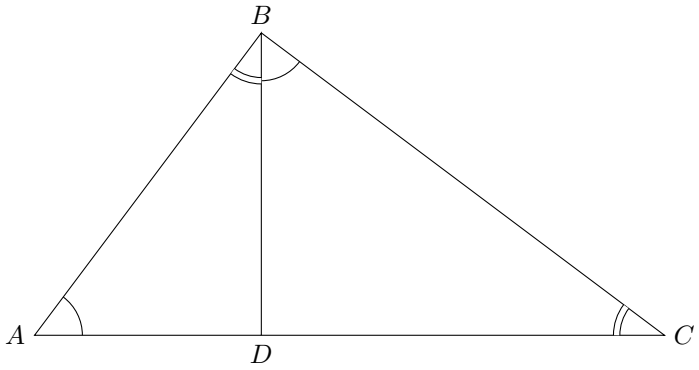
triangles. So he found a new proof, not altogether different from the earlier proof yet without its flaw.

Young Archimedes

> "There!" he said triumphantly, and straightened himself up to look at them. "Now I'll explain".
>
> And he proceeded to prove the theorem of Pythagoras—not in Euclid's way, but by the simpler and more satisfying method which was, in all probability, employed by Pythagoras himself. He had drawn a square and dissected it, by a pair of crossed perpendiculars, into two squares and two equal rectangles. The equal rectangles he divided up by their diagonals into four equal right-angled triangles. The two squares are then seen to be the squares on the two sides of any of these triangles other than the hypotenuse. So much for the first diagram. In the next he took the four right-angled triangles into which the rectangles had been divided and rearranged them round the original square so that their right angles filled the corners of the square, the hypotenuses looked inwards, and the greater and lesser sides of the triangles were in continuation along the sides of the squares (which are equal to the sum of these sides). In this way the original square is redissected into four right-angled triangles and the square on the hypotenuse. The four triangles are equal to the two rectangles of the original dissection. Therefore the square on the hypotenuse is equal to the sum of the two squares—the squares on the two other sides—into which, with the rectangles, the original square was first dissected.



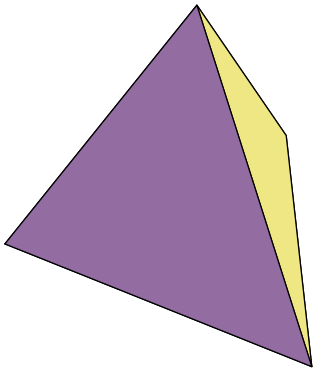




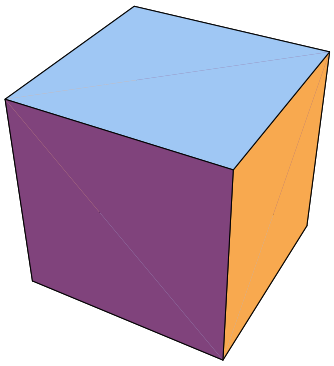
$$\frac{AD}{AB} = \frac{AB}{AC} \implies AD \cdot AC = AB^2$$
$$\frac{DC}{BC} = \frac{BC}{AC} \implies DC \cdot AC = BC^2$$

Thus

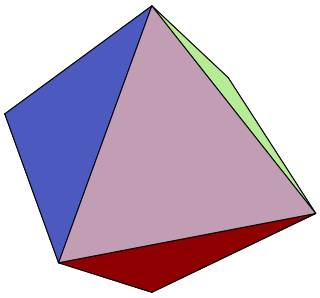
$$AB^2 + BC^2 = AD \cdot AC + DC \cdot AC = AC^2$$



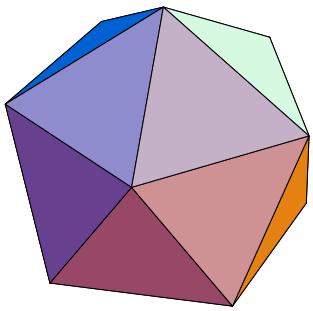
TETRAHEDRON/FIRE



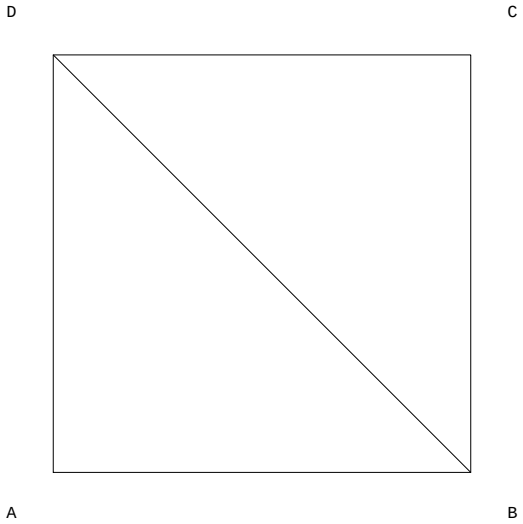
CUBE/EARTH



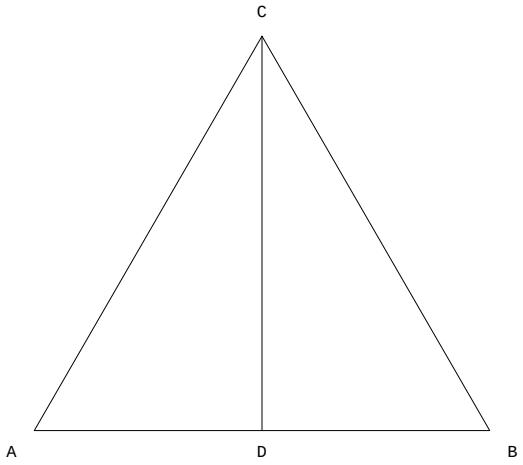
OCTAHEDRON/AIR



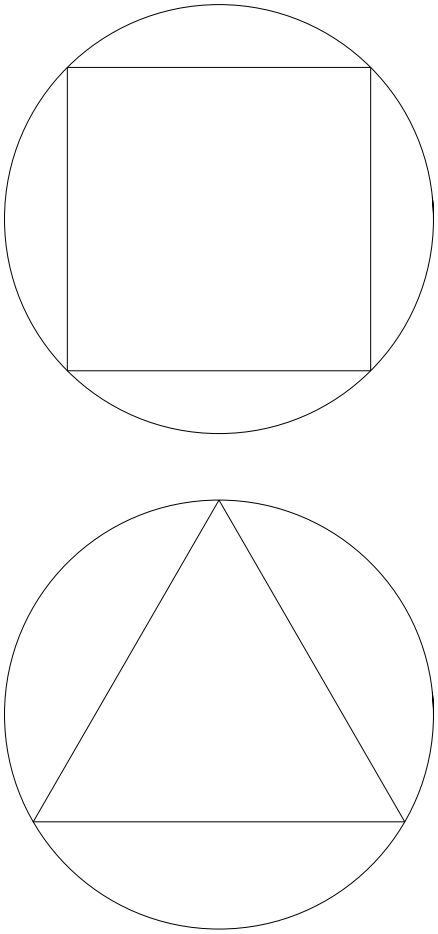
ICOSAHEDRON/WATER

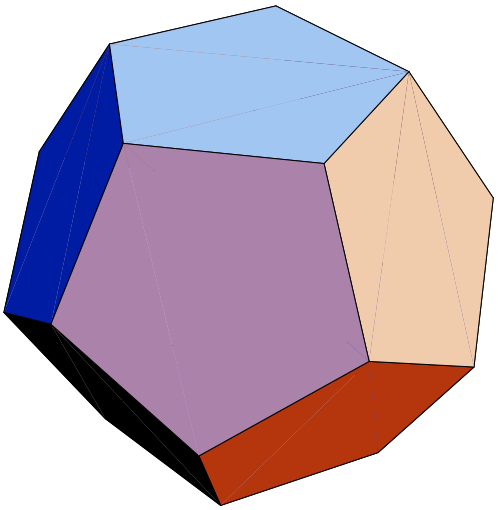


$$DB : AB = \sqrt{2} : 1$$



$$CD : AB : AD = \sqrt{3} : 2 : 1, \quad (\sqrt{3})^2 + 1 = 2^2$$





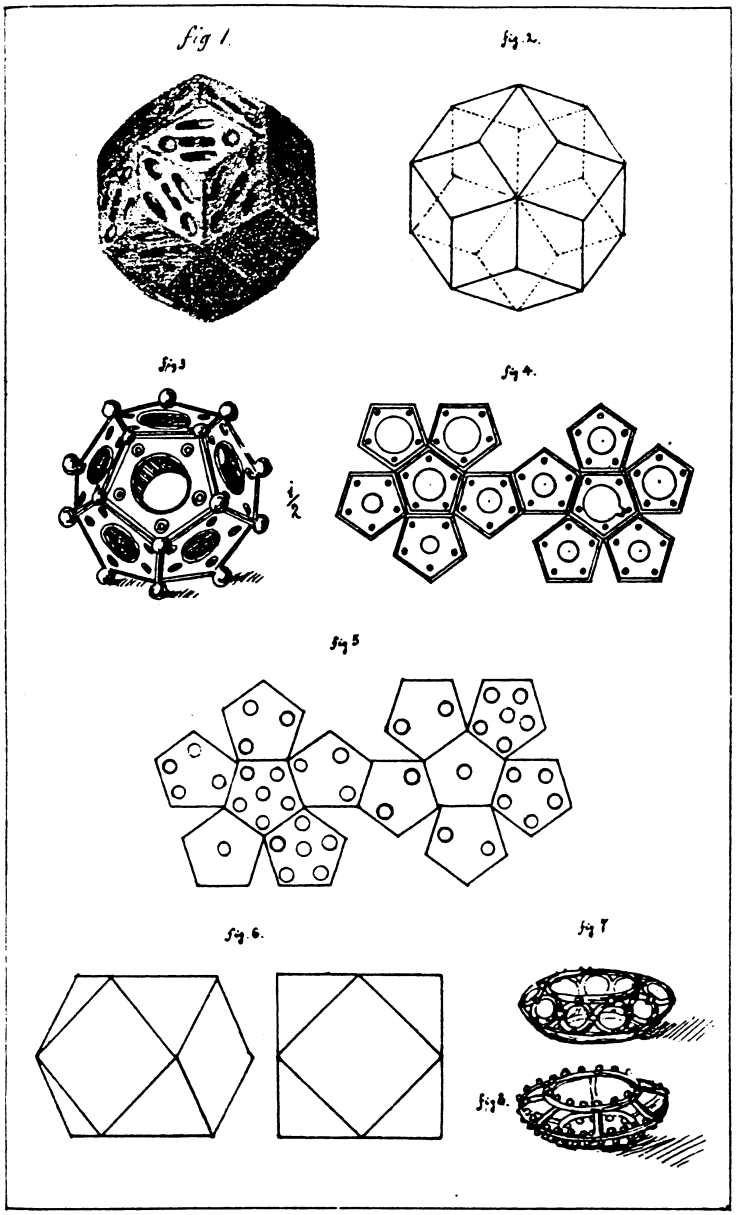
DODECAHEDRON

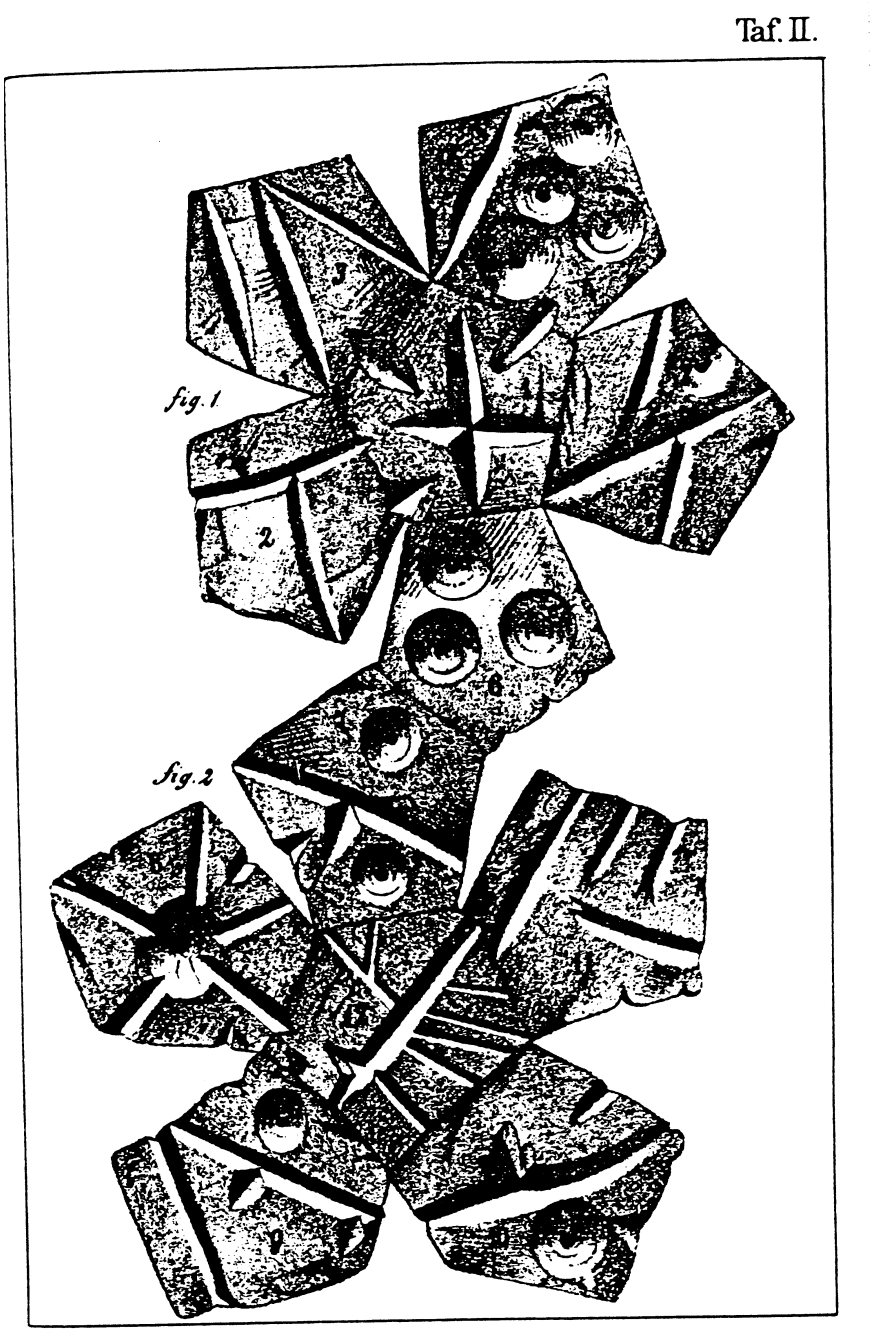
The Dodecahedron and the Celts

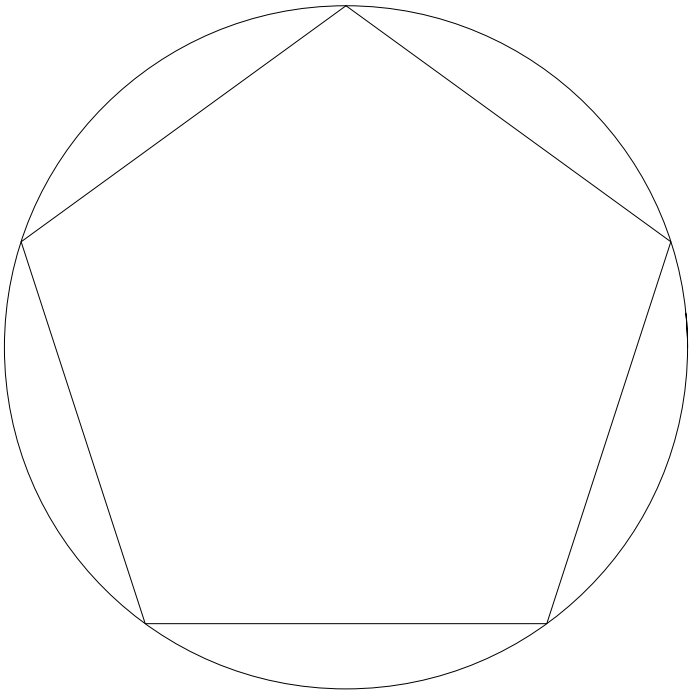
The use of the pentagon as an artistic motif was apparently extremely, extremely rare, and it appears, although I have made no serious attempt to examine the literature, that the dodecahedron as an artistic motif was almost entirely confined to the Celts, and perhaps the Etruscans, during the first half of the first millennium before Christ. It has been proposed. with good reason, that it was suggested to the Celts, for whom the smelting of iron was very important, by the form of iron pyrite crystals, which is approximately but not exactly dodecahedronal. That would contradict the laws of crystallography. Hermann Weyl in his book on symmetry observes that radiolarians appear with dodecahedral symmetry, but since they are minute marine creatures, it is unlikely that they had come to the attention of the Celts.

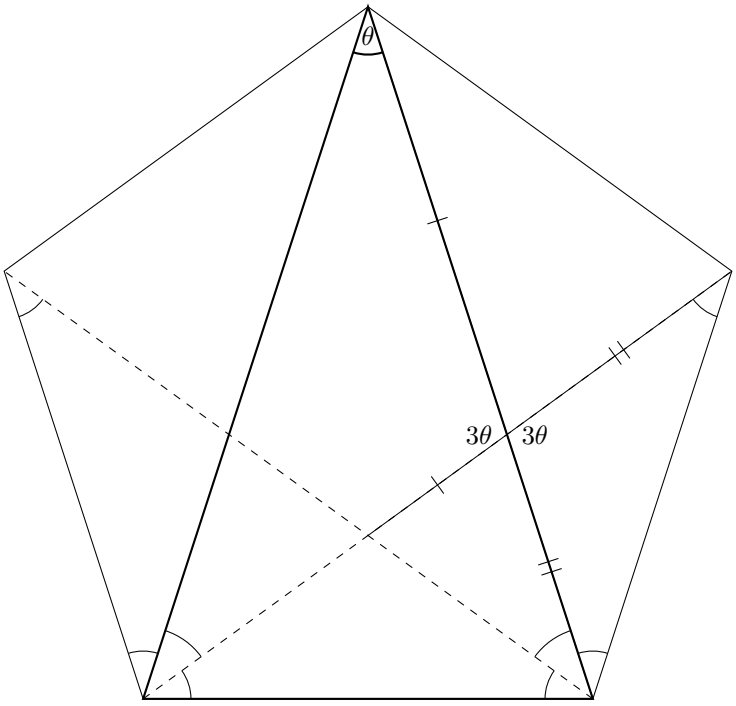
It has also been suggested that Pythagoras who spent some time in Italy may have had some contact with the Celts or with Etruscans and may have been introduced by them to the dodecahedron.

Taf. I.



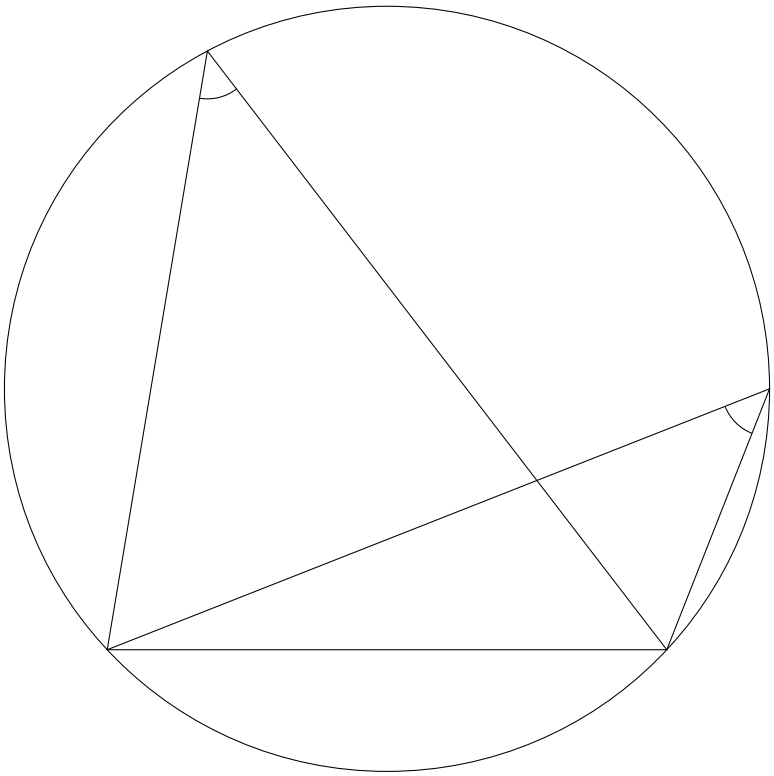

Taf. II.
fig. 1
fig. 2



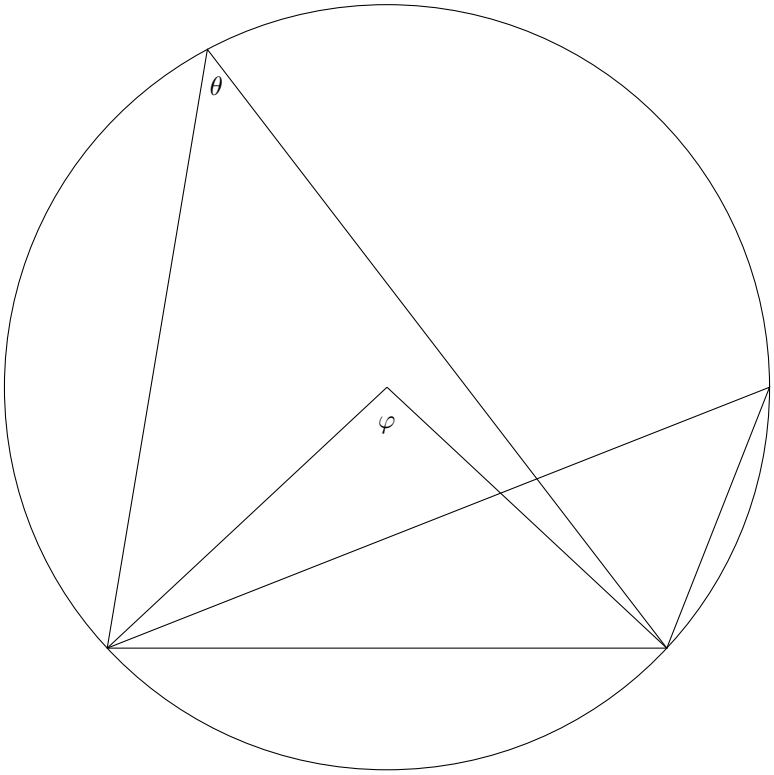

θ
3θ
3θ

$$\begin{aligned} \theta + 2\theta + 2\theta &= 180^\circ \\ 5\theta &= 180^\circ \\ \theta &= 36^\circ \end{aligned}$$

$$\begin{aligned} 5\theta &= \pi \\ \theta &= \frac{\pi}{5} \end{aligned}$$

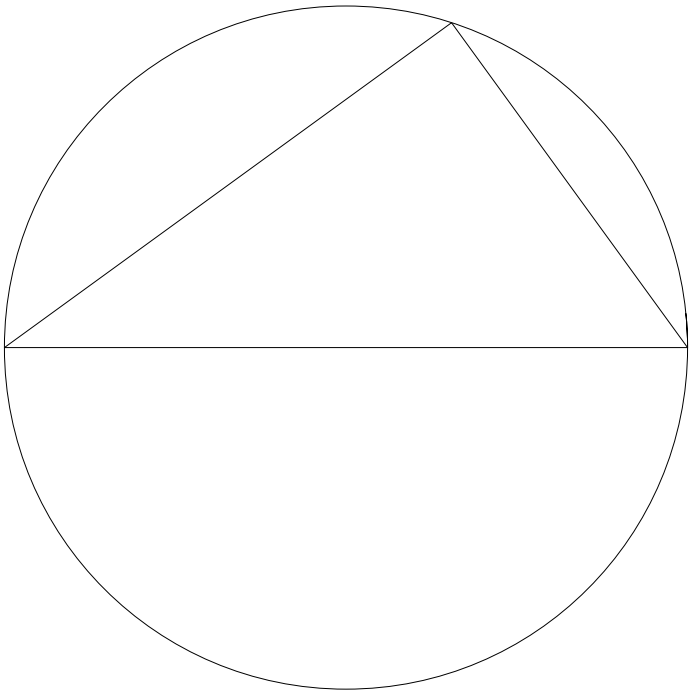


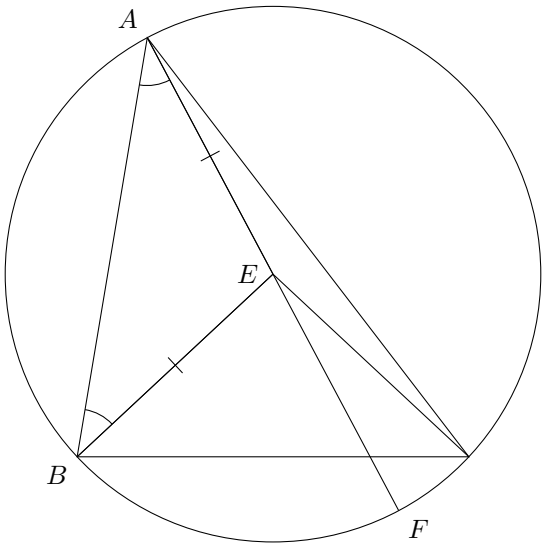
Lecture 3

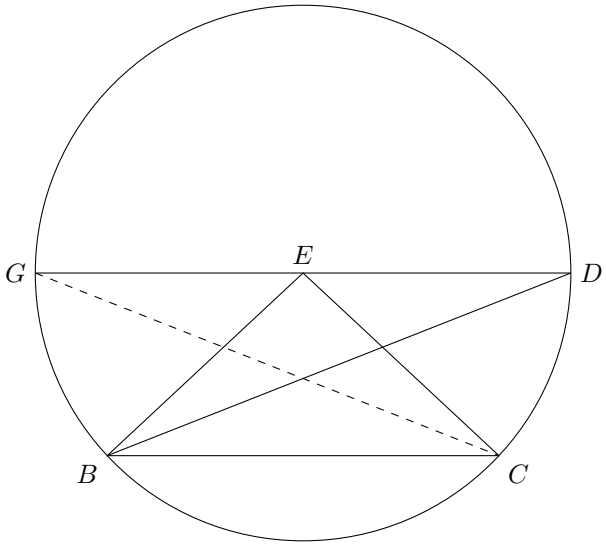


$\varphi = 2\theta$

Date of lecture: Fall term, November 9, 1999.




A
E
B
F

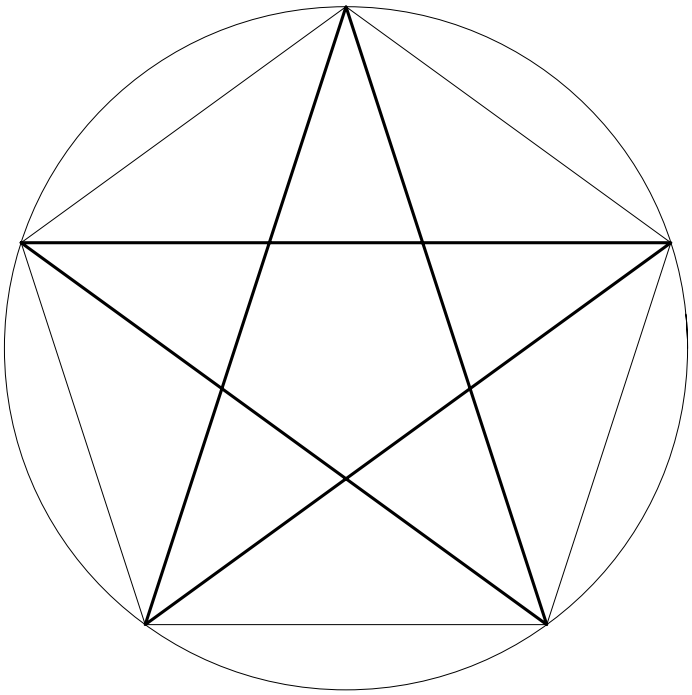

G
E
D
B
C

$$2\angle EAB = \angle EAB + \angle EBA$$
$$\angle EAB + \angle EBA + \angle BEA = 2 \text{ right angles}$$
$$\angle FEB + \angle BEA = 2 \text{ right angles}$$

$$\implies \angle FEB = 2\angle EAB$$

$$\angle GEC = 2\angle GDC$$
$$\angle GEB = 2\angle GDB$$

$$\implies \angle BEC = 2\angle BDC$$



Reminder

Our ultimate purpose over the course of the year is to acquire a feeling for modern number theory, especially for a few of the many conjectural links between algebraic irrationalities on the one hand and, on the other, the Riemann zeta function and, implicitly, various similar functions. The rogue's yarn that will run through much of the material is the algebraic symmetry to which the name of Galois is attached and which I wanted to introduce in as concrete and appealing a way as possible, and in a way that linked it, in a certainly anachronous but not entirely factitious manner, with classical mathematics.

Apart from its intrinsic appeal, that is the reason for treating the construction of the pentagon, and our task today will be to acquire some feel for this construction. It is not easy. So we have to spend an hour on difficult mathematics. You should not be discouraged if you don't understand everything. What follows, namely the basic notions of analytic or Cartesian geometry, will be a little duller, but easier.

It is generally accepted that the subject of modern algebra was born during the Renaissance and analytic geometry, at least the treatment of Descartes, would have been unthinkable without the new algebraic methods. Among other things, it was understood during this period how to solve cubic equations and quartic equations. I could have used them as an introduction to the algebraic symmetry, but decided that a geometrical introduction would be more appealing.

The construction of the triangle

Proposition IV.10. *To construct an isosceles triangle having each of the angles at the base double of the remaining one.*

This proposition is a result of several others from which I single out the three most important.

Proposition II.11. *To cut a given line so that the rectangle contained by the whole and one of the segments is equal to the square on the remaining segment.*

Proposition III.37. *If a point be taken outside a circle and from the point there fall on the circle two straight lines, if one of them cut the circle, and the other fall on it, and if further the rectangle contained by the whole of the straight line which cuts the circle and the straight line intercepted on it outside between the point and the convex circumference be equal to the square on the straight line which falls on the circle, the straight line which falls on it will touch the circle.*

Proposition III.32. *If a straight line touch a circle, and from the point of contact there be drawn across, in the circle, a straight line cutting the circle, the angles which it makes with the tangent will be equal to the angles in the alternate segments of the circle.*

With this proposition we are in the fourth book of the Elements. The Pythagorean theorem is Proposition I.47, and is thus from the first book. There are thirteen books in all, but the propositions that we need come from the first four, which are all geometric in content. Book I contains the most familiar material, ending with the Pythagorean theorem. Book II, to which we shall have to return for some propositions, deals with what is sometimes called geometrical algebra, thus with material that is somewhat perplexing to a modern reader, as familiar algebraic operations are clothed in very unfamiliar geometric garb. Book III deals by and large with properties of circles that have, even for us, an appealing geometric meaning. We shall need some of them, too, so that we shall acquire some familiarity with these two books at first hand. Book IV deals with the inscription of polygons in a circle, starting with the more elementary and familiar case of an arbitrary triangle and a square. I observe in passing the difference. An arbitrary triangle can be inscribed in a circle, but not all quadrilaterals can. Finally it is shown how to inscribe in a circle a regular pentagon, a regular hexagon, and a regular pentadecagon, with fifteen sides. To inscribe a hexagon is easy. The construction is probably known to all of you. The regular pentadecagon is easily dealt with once the triangle and the pentagon are inscribed. Thus our aim is to reach the end of the fourth book. We shall go no further in Euclid for the moment, but it may be useful to review briefly the contents of the remaining books.

The fifth book has quite a different character. It treats Eudoxus's theory of proportions. The sixth book treats, on the basis of Book V, largely of similar figures, especially of similar triangles, and thus contains material that is either intuitively familiar or familiar from school geometry, where it will have been treated without the explicit help of the theory of proportions. Books VII, VIII and IX treat of numbers and number theory, especially of prime numbers, so that we may have occasion to return to them, explicitly or implicitly.

From the point of view of our later algebraic analysis of Euclidean constructions, Book X is the most interesting. We shall show that Euclidean constructions amount, in algebraic terms, to repeatedly adding, subtracting, multiplying and dividing numbers and repeatedly forming their square roots. This book studies, entirely in geometrical terms, the numbers so obtained. I give some examples from Heath's notes to the book. Our purpose is not to study a large number of specific examples or to study the examples in exclusively geometric terms, but to understand why Euclid's constructions lead only to square roots, and what can be constructed using nothing but square roots, and no other surds or algebraic irrationalities.

Books XI, XII, and XIII are about three-dimensional geometry, but are quite different. Book XI treats lines and planes in three-space, thus what we would call the affine geometry of three-space, usually treated in courses on linear algebra, up to and including volumes of parallelograms. Book XII uses especially the method of exhaustion to treat areas and volumes of other, less simple plane figures and solid volumes, for example, circles (disks!) and spheres. Finally, Book XIII treats the construction and the properties of the five regular, or Platonic, solids. This is, among other things, a much deeper, or if you like more elaborate, analysis of various quadratic irrationalities, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, that we have already encountered. Thus it is not unrelated to Book X.

$$\sqrt{a\sqrt{B}}$$

$$\sqrt[4]{AB} = \sqrt{\sqrt{AB}}$$

$$\sqrt{a^2 - \frac{k^2a^2}{1+k^2}}$$

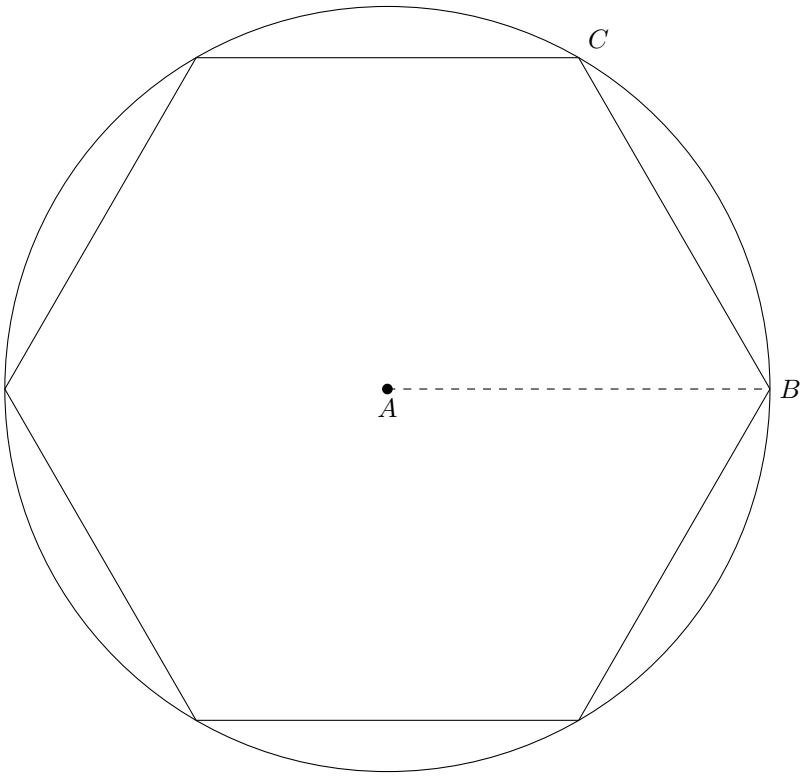
$$\frac{A - k^2A}{\sqrt[4]{A(A-k^2A)}}$$

$$\frac{\rho}{\sqrt{2}}\sqrt{1 - \frac{k}{\sqrt{1+k^2}}}$$

$$\frac{\rho}{\sqrt{2(1+k^2)}}\sqrt{\sqrt{1+k^2}+k} + \frac{\rho}{\sqrt{2(1+k^2)}}\sqrt{\sqrt{1+k^2}-k}$$

$$\frac{\rho\lambda^{1/4}}{\sqrt{2}}\sqrt{1 + \frac{k}{\sqrt{1+k^2}}} + \frac{\rho\lambda^{1/4}}{\sqrt{2}}\sqrt{1 - \frac{k}{\sqrt{1+k^2}}}$$

Hexagon



$AB = BC$

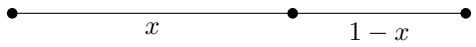
Proposition II.11. *To cut a given line so that the rectangle contained by the whole and one of the segments is equal to the square on the remaining segment.*

This reappears in Book VI as Proposition VI.30, but after the theory of proportions has been established in Book V.

Proposition VI.30. *To cut a given line in extreme and mean ratio.*

I recall the definition.

Definition VI.3. *A straight line is said to have been cut in extreme and mean ratio when, as the whole line is to the greater segment, so is the greater to the less.*



Thus

$$\frac{1}{x} = \frac{x}{1-x} \implies 1 - x = x^2 \implies x^2 + x - 1 = 0 \implies x = \frac{-1 \pm \sqrt{5}}{2}$$

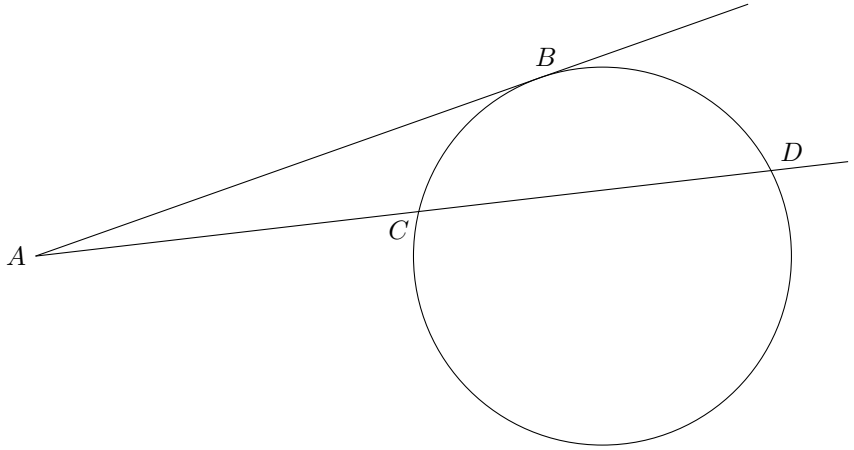
Since x is positive

$$x = \frac{\sqrt{5}-1}{2} \implies \frac{x}{1-x} = \frac{\sqrt{5}+1}{2}$$ Golden Section

Proposition III.37. *If a point be taken outside a circle and from the point there fall on the circle two straight lines, if one of them cut the circle, and the other fall on it, and if further the rectangle contained by the whole of the straight line which cuts the circle and the straight line intercepted on it outside between the point and the convex circumference be equal to the square on the straight line which falls on the circle, the straight line which falls on it will touch the circle.*

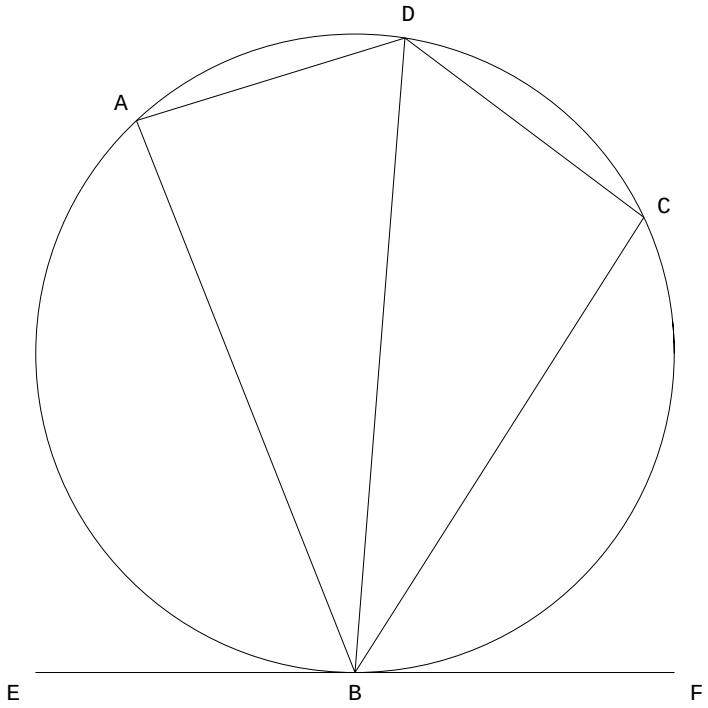
This proposition is the converse to the following one, the one I shall prove.

Proposition III.36. *If a point be taken outside a circle and from it there fall on the circle two straight lines, and if one of them cut the circle and the other touch it, the rectangle contained by the whole of the straight line which cuts the circle and the straight line intercepted on it outside between the point and the convex circumference will be equal to the square on the tangent.*



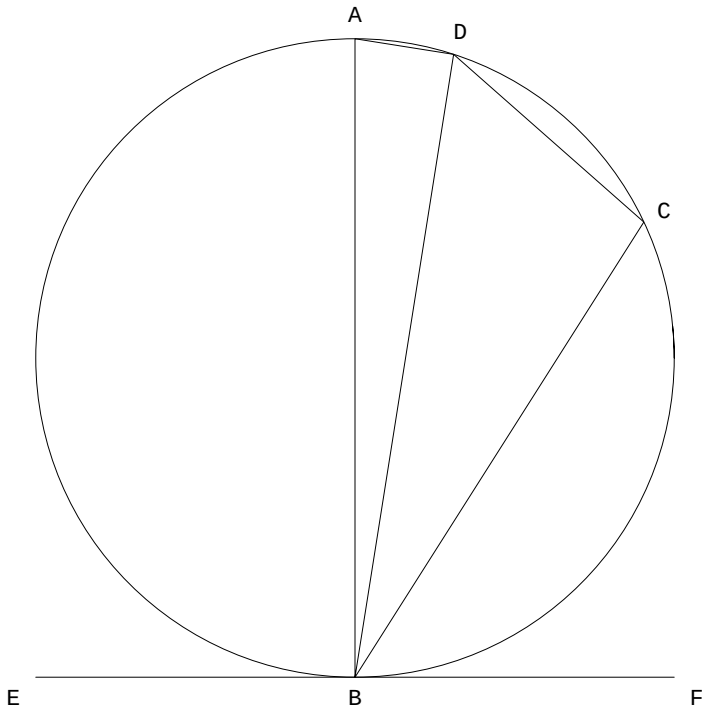
$$AC \cdot AD = AB^2$$

Proposition III.32. *If a straight line touch a circle, and from the point of contact there be drawn across, in the circle, a straight line cutting the circle, the angles which it makes with the tangent will be equal to the angles in the alternate segments of the circle.*



$$\angle FBD = \angle BAD, \quad \angle EBD = \angle BCD$$

Proof



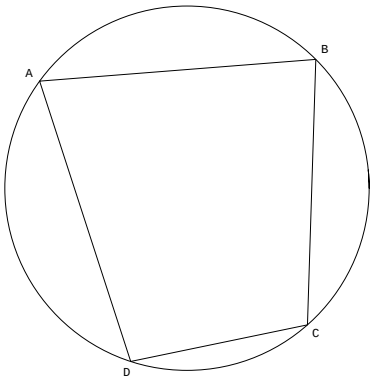
$$\angle ADB = \square \implies \angle BAD + \angle ABD = \square$$
$$\angle ABF = \square \implies \angle FBD + \angle DBA = \square$$

Thus

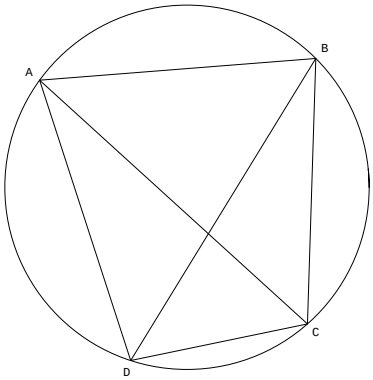
$$\angle BAD = \angle FBD \implies \angle EBD = \angle BCD$$

Supplement to proof

Proposition III.22. *The opposite angles of quadrilaterals in circles are equal to two right angles*



Add two lines to the diagram.

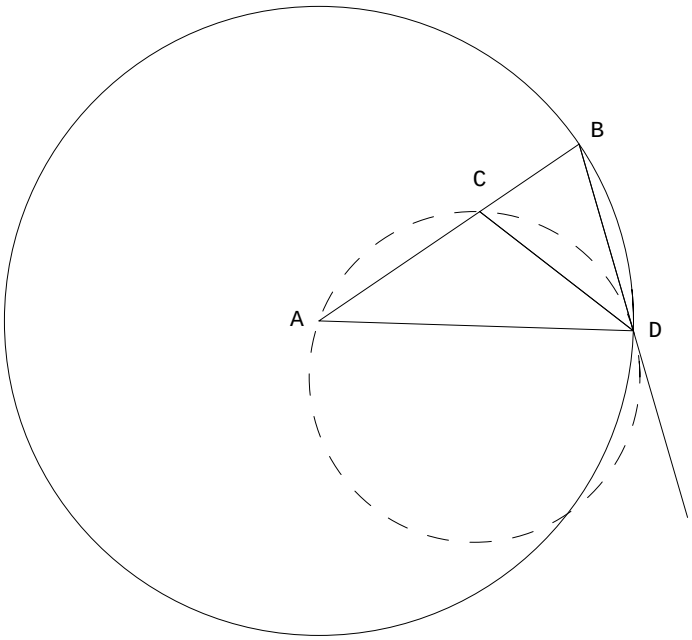


$$\angle CAB = \angle BDC$$
$$\angle ACB = \angle ADB$$

$$\implies \angle ADC = \angle BAC + \angle ACB$$
$$\implies \angle ABC + \angle ADC =$$
$$\angle ABC + \angle BAC + \angle ACB = 2\square$$

Construction

Take a segment AB and divide it by a point C so that $AB : AC = AC \div CB$. Draw a circle with center A passing through B and choose D so that $BD = AC$. The desired triangle is ABD.



$$AC = BD, \quad AB \cdot BC = AC^2 \implies AB \cdot BC = BD^2$$

Thus BD touches the circle ACD. Moreover $\angle BDC = \angle DAC$. Therefore

$$\angle CBD = \angle BDA = \angle BDC + \angle CDA = \angle DAC + \angle CDA = \angle BCD$$

Thus $CD = BD = AC$ so that $\angle CAD = \angle ADC$ and $\angle BCD = 2 \times \angle CAD$.

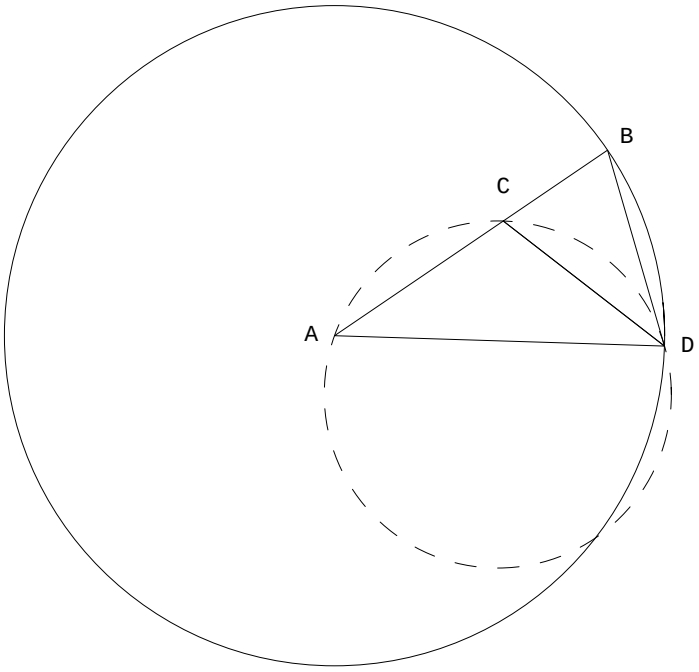
But $\angle BCD = \angle BDA = \angle ABD$.

The construction backward

Suppose the triangle ABD is given with the property that

$$\angle BDA = \angle DBA = 2 \times \angle DAB.$$

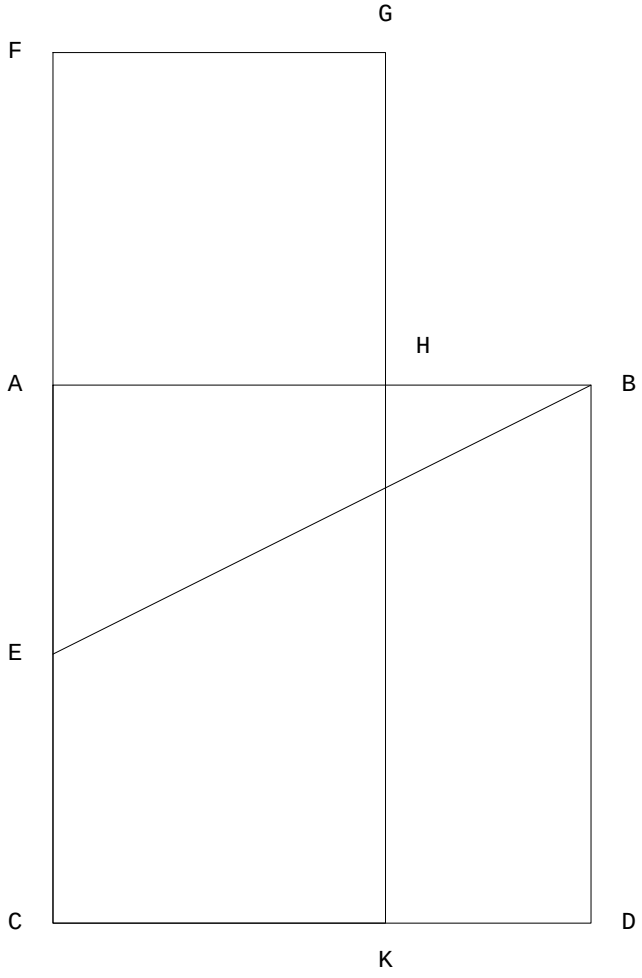
Bisect BDA. Then $BD = DC = CA$. BD must touch the circle ACD so that $AC^2 = BD^2 = BC \cdot BA$.



Proposition II.11

Proposition II.11. *To cut a given line so that the rectangle contained by the whole and one of the segments is equal to the square on the remaining segment.*

Let AB be the given line. Describe the square $ABCD$ on AB. Bisect AC at E and join E to B. (Note that if $AB = 1$ then $EB = \sqrt{1^2 + 1/2^2} = \sqrt{5}/2$.) Let EF be made equal to BE. Draw the square FH on AF. (Then $AH = FA = \sqrt{5}/2 - 1/2$.)



Proposition II.11—continued

As a first step we need that

$$CF \cdot FA + AE^2 = EF^2 \qquad \left((y+1)\cdot y + \frac{1}{2^2} = \left(y + \frac{1}{2}\right)^2\right)$$

This is Proposition II.6 and will be proved separately.

$$EF^2 = EB^2 = AE^2 + BA^2 \implies CF \cdot FA = BA^2$$

$$FA = FG \implies FK = AD \qquad \text{(Areas)}$$

Subtract AK from each. Then $FH = HD$. The rectangle contained by AB, BH is equal to the square on HA.

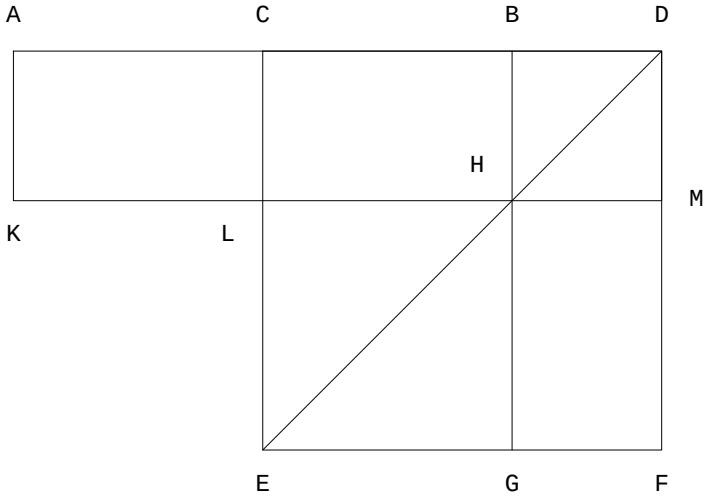
Proposition II.6. *If a straight line be bisected and a straight line be added to it in a straight line, the rectangle contained by the whole with the added straight line and the added straight line together with the square on the half is equal to the square on the straight line made up of the half and the added straight line.*

This is the relation

$$(x+y)\cdot y + \frac{x^2}{2^2} = \left(y + \frac{x}{2}\right)^2$$

AB $(= x)$ is bisected at C and BD $(= y)$ is added to it in a straight line. To be shown that

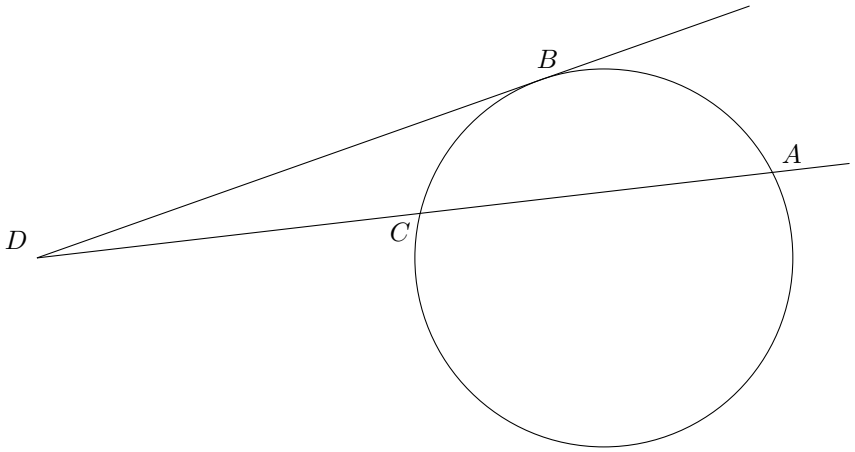
$$AD \cdot DB + CB^2 = CD^2$$



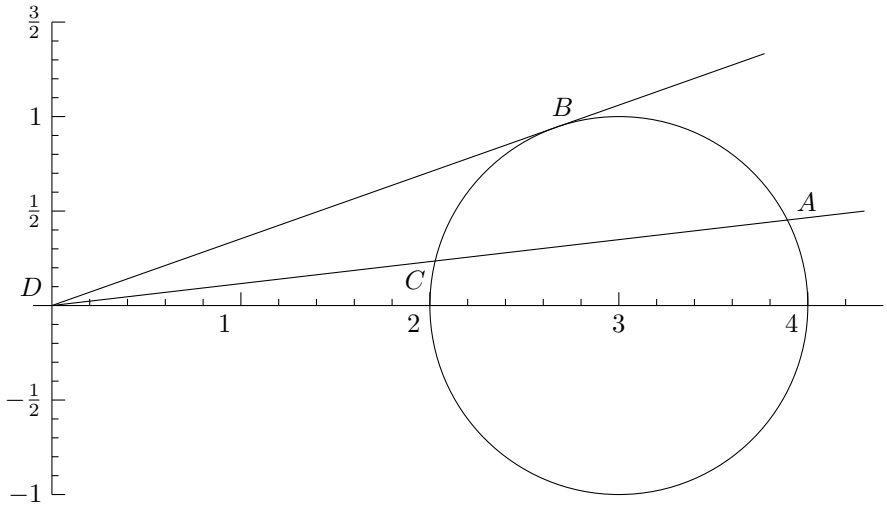
Draw the square $CEFD$; join DE and draw BG parallel to DF and KM through H parallel to AD. Thus $AL = CH = HF$. Adding CM, we have

$$AM = \text{Gnomon}\, CDF$$

Thus the rectangle AD, BD is equal to the gnomon CDF and the rectangle AD, BD together with the square on CB is equal to the gnomon plus LG, thus to the square on CD.



I introduce coordinates.



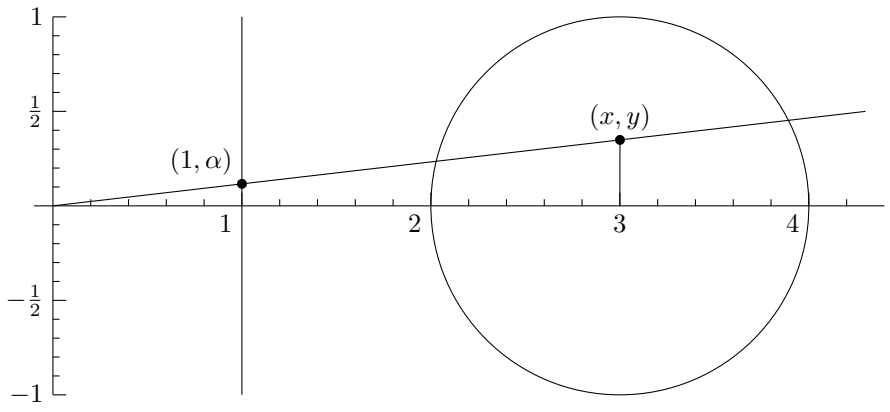
D at $(0, 0)$; center at $(a, 0)$; radius is r; $C = (x_1, y_1)$, $A = (x_2, y_2)$

$$DC = \sqrt{x_1^2 + y_1^2} \quad DA = \sqrt{x_2^2 + y_2^2}$$

The proposition implicitly affirms that

$$DC \cdot DA = \sqrt{x_1^2 + y_1^2}\sqrt{x_2^2 + y_2^2}$$

is independent of line, provided that it falls on the circle, so that this number equals its value in the extreme case that $A = C$, thus is equal to DB^2.



$$\frac{\alpha}{1} = \frac{y}{x}$$

Suppose $(1,\alpha)$ is the point where the line $x = 1$ crosses the line DA. By the theory of similar triangles, a point (x,y) lies on the line exactly when it is of the form $(x,y) = (x,\alpha x)$, thus $y = \alpha x$. Both (x_1,y_1) and (x_2,y_2) are solutions of the equation

$$(x-a)^2 + y^2 = r^2 \quad \text{or} \quad (x-a)^2 + \alpha^2 x^2 = r^2$$

or

$$x^2 - 2ax + a^2 + \alpha^2 x^2 = r^2 \quad \text{or} \quad (1+\alpha^2)x^2 - 2ax + a^2 - r^2 = 0$$

Recall

$$Ax^2 + Bx + C = 0$$

has solutions

$$x_2 = \frac{-B + \sqrt{B^2 - 4AC}}{2A}, \quad x_1 = \frac{-B - \sqrt{B^2 - 4AC}}{2A}$$

Thus

$$x_1 x_2 = \frac{B^2 - B^2 + 4AC}{4A^2} = \frac{C}{A}$$

Since $y_1 = \alpha x_1$ and $y_2 = \alpha x_2$,

$$\sqrt{x_1^2 + y_1^2} = \sqrt{1+\alpha^2}x_1, \quad \sqrt{x_2^2 + y_2^2} = \sqrt{1+\alpha^2}x_2$$

$$\sqrt{x_1^2 + y_1^2}\sqrt{x_2^2 + y_2^2} = (1+\alpha^2)x_1 x_2 = (1+\alpha^2)\frac{a^2 - r^2}{1+\alpha^2} = a^2 - r^2.$$

Solve:

$$ax^2 + bx + c = 0$$

Complete the square.

$$a\left(x^2 + 2\frac{bx}{2a} + \frac{b^2}{4a^2}\right) + \left(c - \frac{b^2}{4a}\right) = a\left(x^2 + 2\frac{bx}{2a} + \frac{b^2}{4a^2}\right) + \frac{(4ac - b^2)}{4a} = 0$$

We divide by a.

$$\left(x^2 + 2\frac{bx}{2a} + \frac{b^2}{4a^2}\right) + \frac{(4ac - b^2)}{4a^2} = \left(x + \frac{b}{2a}\right)^2 + \frac{(4ac - b^2)}{4a^2} = 0$$

Thus

$$x + \frac{b}{2a} = \pm\frac{\sqrt{b^2 - 4ac}}{2a}$$

or

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Lecture 4

TODAY'S TASK

To understand the relation between the Euclidean geometrical constructions and algebra, especially addition, subtraction, multiplication, division, and the extraction of square roots.

Date of lecture: Fall term, November 16, 1999.

The historical development of Cartesian geometry took place over about a century and a half, from the middle of the sixteenth to the end of the seventeenth, and was neither begun by Descartes nor ended by him. His concerns were none the less to some extent ours, the discovery and analysis of geometric constructions by algebraic means. On the other hand, the use of a rectilinear coordinate system, so familiar to us from various cities, especially New York, is not to be found in Descartes, where indeed one does not see a coordinate system at all. Descartes published his views early in the seventeenth century. Coordinate systems in a sense approximating ours did not appear until late in the century, in particular, in the works of Newton and Leibniz.

Nevertheless Descartes's concerns are closer to ours than are those of other authors, whom I am in any case not yet in a position to discuss. Descartes not only published in the vernacular but also has been widely translated, so that he is much more accessible than many of the others.

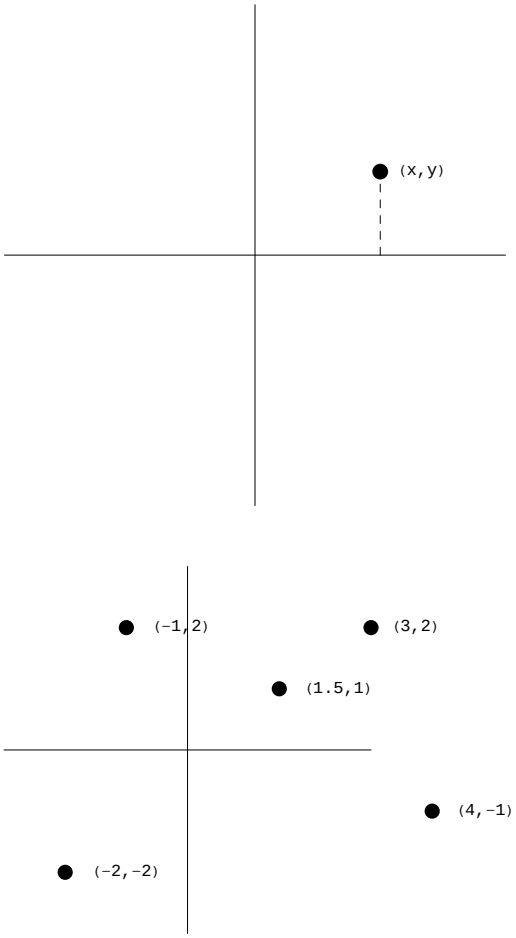
Since some familiarity with coordinate systems and their manipulation is almost universal in the modern world, it will be most efficient to be quite ahistorical and to run through a standard, textbook treatment, so that we can get on to Gauss within a reasonable time. Even so a few scattered references to Descartes will be useful, just for fun.

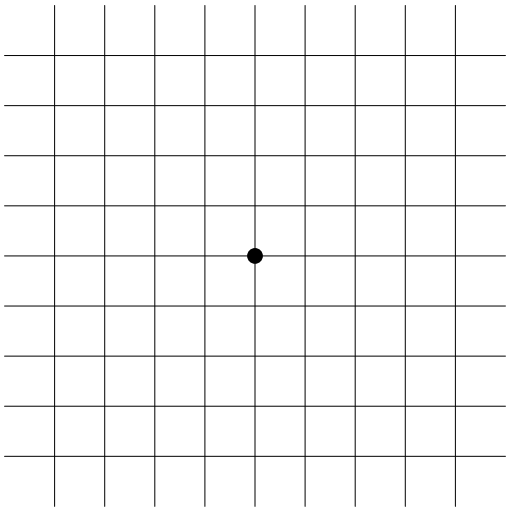
We shall have to analyze algebraically the constructions of Euclidean geometry, thus analyze these constructions in terms of Cartesian geometry. We examine first translation and rotation. Once the coordinates are chosen, we can consider translation by a *given* (a, b), thus translation by a parallel to one axis and then by b parallel to another, where it is understood that a or b could be negative, thus comprise both a magnitude and a direction and that then we are to translate to the left or downward. Consider the first step. To translate the point (x, y) parallel to the horizontal axis, thus parallel to the axis of abscissas, we draw a line through $p = (x, y)$ parallel to this axis, a construction that, according to Euclid, can be carried out with a ruler and compass. Then with the help of a compass, we mark on it a point to the right or left of p, according to the sign of a, that is at a distance from it equal to the magnitude of a. The second translation is effected in a similar fashion. In particular, therefore, the constructions of Euclidean geometry allow us to add or subtract two numbers, which could be, for example, a and x.

Multiplication is a different matter, because there is a philosophical point to discuss first. In Cartesian geometry we have a fundamental length, so that it is appropriate to identify lengths and numbers. We can therefore add two lengths or two numbers, and scarcely notice the difference. Multiplying two lengths yields however an area, which is not yet identified with a number, so that we have to be careful. We should therefore be explicit about the fundamental length. We call it λ. Then another length is μ and it is only μ/λ that is a number, a proportion or a ratio in the language of Euclid. How then do we multiply two proportions μ/λ and ν/λ? We use similar triangles. We can divide in a similar way. All we need is exchange the roles of ν and η.

Since rotation is an operation that can, as we have seen, be carried out by multiplying coordinates, rotation of a given point, and thus of a given line, determined by any two points on it, can be carried out explicitly provided that the angle is given, either by its sine and cosine or by the two lines that form it, for from them the sine and cosine can be determined.

Cartesian or analytic geometry

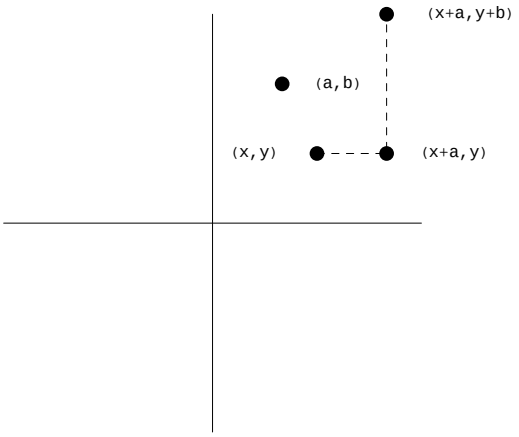




Observe that in Cartesian geometry a length is only implicit, or if one prefers there is no length, it has been replaced by a pure number. Thus in Cartesian geometry the notion of number is primary and independent of length, whereas in euclidean geometry the notion of number is secondary and is derived from that of length.

The notion of *congruence* that is so essential for Euclidean geometry has now to be made explicit as a combination of *translations* and *rotations*. I recall the formulas.

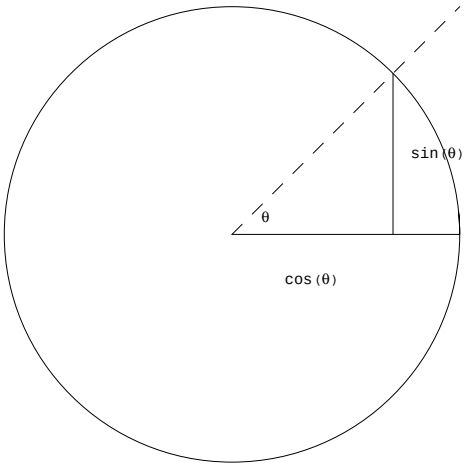
Translation



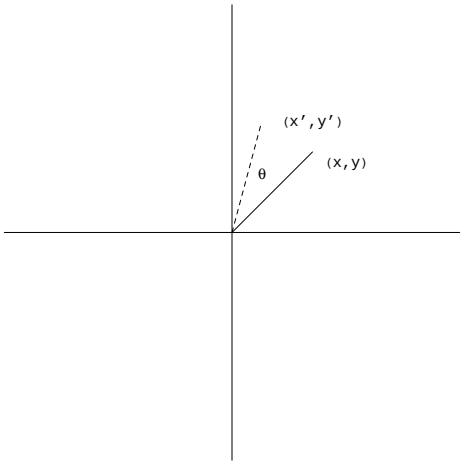
Rotation

Rotation is more difficult. Recall that rotation of a figure and especially of a point is a turning about some given point that we can take at first to be the origin.

A rotation is through an *angle* and we have first to be able to specify an angle. This is done—as you will no doubt be delighted to discover—through its sine and cosine.

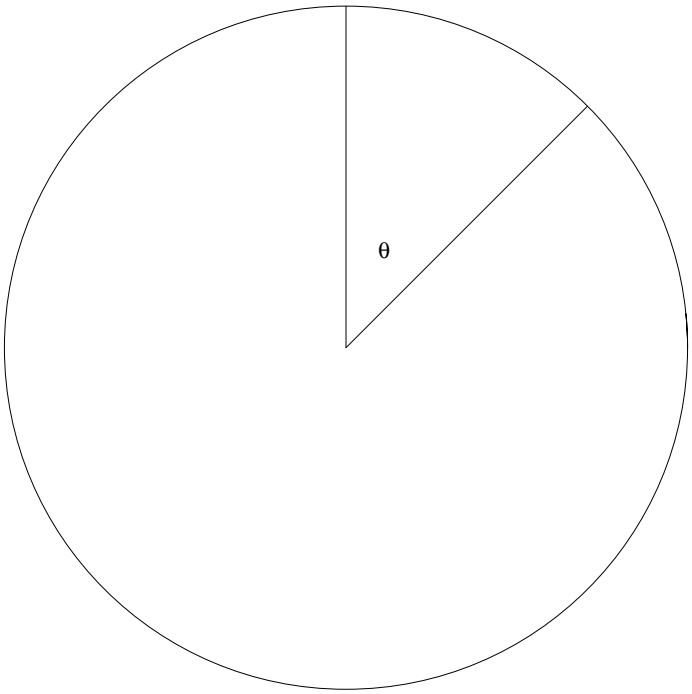


We want to rotate.

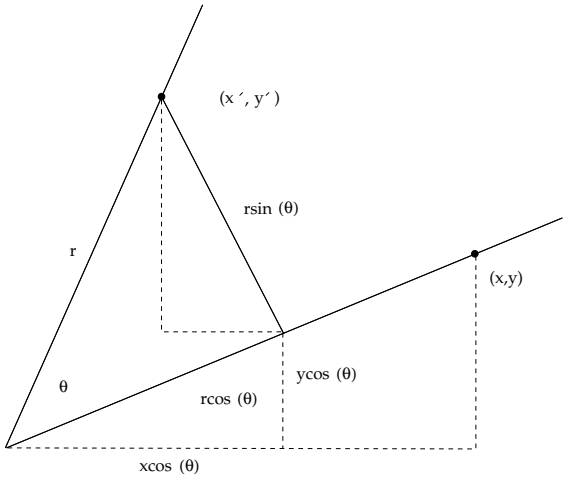


How do we find the coordinates (x', y') in terms of (x, y)?

Measurement of angles



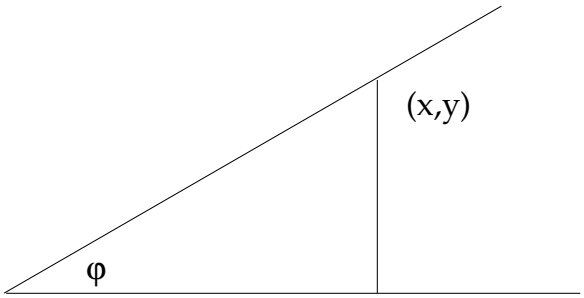
An angle is normally measured by the length of the arc it subtends. This length can be measured in two different units: degrees or radians. Degrees are defined by the condition that the total circumference have length 360° and radians by the condition that the total circumference have length 2π, thus by the condition that the radius have length 1. We shall use radians as our measure. A right angle contains 90° or $\pi/2$ radians.



The point (x, y) is at a distance $r = \sqrt{x^2 + y^2}$ from the origin, about which we are rotating. There are two triangles in the figure similar to the triangle with vertices $(0, 0)$, $(x, 0)$, (x, y), a triangle which itself is not shown. It is right-angled with hypotenuse r, vertical side y and horizontal side x. Of the two triangles, one has hypotenuse $r\cos(\theta)$. The other has hypotenuse $r\sin(\theta)$. The one whose sides are not given has its vertical side equal to $x\sin(\theta)$ and its horizontal side equal to $y\sin(\theta)$.

We are trying to find the coordinates (x', y'). They are seen to be

$$x' = x\cos(\theta) - y\sin(\theta),$$
$$y' = x\sin(\theta) + y\cos(\theta).$$



This is the triangle with vertices $(0,0)$, $(x,0)$, (x,y). Let φ be the indicated angle. Since

$$x = r\cos(\varphi), \quad y = r\sin(\varphi),$$

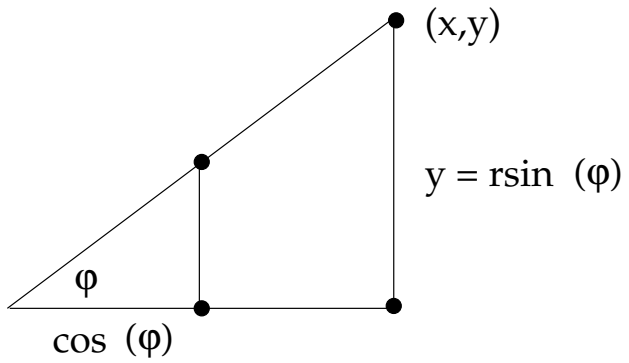
while

$$x' = r\cos(\varphi+\theta), \quad y = r\sin(\varphi+\theta),$$

the formulas on the previous page yield formulas that will be familiar to most of you, but which I recall.

$$\cos(\varphi+\theta) = \cos(\varphi)\cos(\theta) - \sin(\varphi)\sin(\theta),$$
$$\sin(\varphi+\theta) = \cos(\varphi)\sin(\theta) + \sin(\varphi)\cos(\theta).$$

They will be important for us.



rr = xx + yy

Niccolo Tartaglia (c. 1500–1557)

Gerolamo Cardano (1501–1576)

François Viète (1526–1573)

$$ax^3 + bx^2 + cx^2 + d = 0$$
$$ax^4 + bx^3 + cx^2 + dx + e = 0$$

Girard Desargues (c. 1591–1661)

René Descartes (1596–1661)

Pierre de Fermat (1601–1665)

DISCOURS
DE LA METHODE

POUR BIEN CONDUIRE SA RAISON ET CHERCHER
LA VERITÉ DANS LES SCIENCES

Si ce diſcours ſemble trop long pour eſtre tout leu en vne fois, on le pourra diſtinguer en ſix parties. Et, en la premiere, on trouuera diuerſes conſiderations touchant les ſciences. En la ſeconde, les principales regles de la Methode que l'Autheur a cherchée. En la 3, quelques vnes de celles de la Morale qu'il a tirée de cete Methode. En la 4, les raiſons par leſquelles il prouue l'exiſtence de Dieu & de l'ame humaine, qui ſont les fondemens de ſa Metaphyſique. En la 5, l'ordre des queſtions de Phyſique qu'il a cherchées, & particulierement l'explication du mouuement du cœur & de quelques autres difficultez qui appartienent a la Medecine, puis auſſy la difference qui eſt entre noſtre ame & celle des beſtes. Et en la derniere, quelles choſes il croit eſtre requiſes pour aller plus auant en la recherche de la Nature qu'il n'a eſté, & quelles raiſons l'ont fait eſcrire.

Le bon ſens eſt la choſe du monde la mieux partagée : car chaſcun penſe en eſtre ſi bien pouruû, que PREMIERE PARTIE.

ceux meſme qui ſont les plus difficiles a contenter en toute autre choſe, n'ont point couſtume d'en deſirer plus qu'ils en ont. En quoy il n'eſt pas vrayſemblable que tous ſe trompent; mais plutoſt cela teſmoigne que la puiſſance de bien iuger, & diſtinguer le vray d'auec le faux, qui eſt proprement ce qu'on nomme le bon ſens ou la raiſon, eſt naturellement eſgale en tous les hommes; et ainſi que la diuerſité de nos opinions ne vient pas de ce que les vns ſont plus raiſonnables que les | autres, mais ſeulement de ce que nous conduiſons nos penſées par diuerſes voyes, & ne conſiderons pas les meſmes choſes. Car ce n'eſt pas aſſez d'auoir l'eſprit bon, mais le principal eſt de l'appliquer bien. Les plus grandes ames ſont capables des plus grans vices, auſſy bien que des plus grandes vertus; et ceux qui ne marchent que fort lentement, peuuent auancer beaucoup dauantage, s'ils ſuiuent touſiours le droit chemin, que ne font ceux qui courent, & qui s'en eſloignent.

Pour moy, ie n'ay iamais preſumé que mon eſprit fuſt en rien plus parfait que ceux du commun; meſme i'ay ſouuent ſouhaité d'auoir la penſée auſſy prompte, ou l'imagination auſſy nette & diſtincte, ou la memoire auſſy ample, ou auſſy preſente, que quelques autres. Et ie ne ſçache point de qualitez que celles cy, qui ſeruent a la perfection de l'eſprit : car pour la raiſon, ou le ſens, d'autant qu'elle eſt la ſeule choſe qui nous rend hommes, & nous diſtingue des beſtes, ie veux croyre qu'elle eſt toute entiere en vn chaſcun, & ſuiure en cecy l'opinion commune des Philoſophes, qui diſent qu'il n'y a du plus & du moins qu'entre les

accidens, & non point entre les *formes,* ou natures, des *indiuidus* d'vne meſme *eſpece.*

Mais ie ne craindray pas de dire que ie penſe auoir eu beaucoup d'heur, de m'eſtre rencontré dés ma ieuneſſe en certains chemins, qui m'ont conduit a des conſiderations & des maximes, dont i'ay formé vne Methode, par laquelle il me ſemble que i'ay moyen d'augmenter par degrez ma connoiſſance, & de l'eſleuer peu a peu au plus haut point, auquel la mediocrité de mon eſprit & la courte durée de ma vie luy pourront permettre d'atteindre. Car i'en ay deſia recueilly de tels fruits, qu'encore qu'aux iugemens que ie fais de moymeſme, ie taſche touſiours de pencher vers le coſté de la defiance, plutoſt que vers celuy de la preſomption; & que, regardant d'vn œil de Philoſophe les diuerſes actions & entrepriſes de tous les hommes, il n'y en ait quaſi aucune qui ne me ſemble vaine & inutile; ie ne laiſſe pas de receuoir vne extreme ſatisfaction du progrés que ie penſe auoir deſia fait en la recherche de la verité, & de conceuoir de telles eſperances pour l'auenir, que ſi, entre les occupations des hommes purement hommes, il y en a quelqu'vne qui ſoit ſolidement bonne & importante, i'oſe croyre que c'eſt celle que i'ay choiſie.

Toutefois il ſe peut faire que ie me trompe, & ce n'eſt peuteſtre qu'vn peu de cuiure & de verre que ie prens pour de l'or & des diamans. Ie ſçay combien nous ſommes ſuiets a nous méprendre en ce qui nous touche, & combien auſſy les iugemens de nos amis nous doiuent eſtre ſuſpects, lorſqu'ils ſont en noſtre faueur. Mais ie ſeray bien ayſe de faire voir, en ce diſ-

Lecture 5

LA GEOMETRIE

LIVRE PREMIER.

Des problefmes qu'on peut conſtruire ſans y employer que des cercles & des lignes droites.

Tous les Probleſmes de Geometrie ſe peuuent facilement reduire a tels termes, qu'il n'eſt beſoin, par aprés, que de connoiſtre la longeur de quelques lignes droites, pour les conſtruire.

Comment le calcul d'Arithmetique ſe rapporte aux operations de Geometrie.

Et comme toute l'Arithmetique n'eſt compoſée que de quatre ou cinq operations, qui ſont : l'Addition, la Souſtraction, la Multiplication, la Diuiſion, & l'Extraction des racines, qu'on peut prendre pour vne eſpece de Diuiſion *; ainſi n'a-t-on autre choſe a faire, en Geometrie, touchant les lignes qu'on cherche, pour les preparer a eſtre connuës, que leur en adiouſter d'autres, ou en oſter; ou bien, en ayant vne

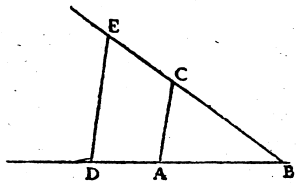
* *Nous indiquons, par des étoiles, les endroits auxquels se rapportent les commentaires de Schooten dans ses éditions latines de la* GEOMETRIE (1649 et 1659). *La lettre de renvoi correspondante est, pour cette page,* A.

Date of lecture: Fall term, November 23, 1999.

que ie nommeray l'vnité* pour la rapporter d'autant mieux aux nombres, & qui peut ordinairement eſtre priſe a diſcretion *, puis en ayant encore deux autres, en trouuer vne quatrieſme, qui ſoit a l'vne de ces deux comme l'autre eſt a l'vnité, ce qui eſt le meſme que la Multiplication *; ou bien en trouuer vné quatrieſme, qui ſoit a l'vne de ces deux comme l'vnité | eſt a l'autre, ce qui eſt le meſme que la Diuiſion *; ou enfin trouuer vne, ou deux, ou pluſieurs moyennes proportionnelles entre l'vnité & quelque autre ligne, ce qui eſt le meſme que tirer la racine quarrée, ou cubique, &c. Et ie ne craindray pas d'introduire ces termes d'Arithmétique en la Geometrie, affin de me rendre plus intelligible.

La Multiplication

Soit, par exemple, AB l'vnité, & qu'il faille multiplier BD par BC; ie n'ay qu'a ioindre les poins A & C, puis tirer DE parallele a CA, & BE eſt le produit de cete Multiplication.

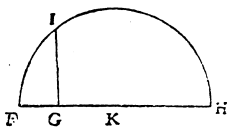


La Diuiſion.

Ou bien, s'il faut diuiſer BE par BD, ayant ioint les poins E & D, ie tire AC parallele a DE, & BC eſt le produit de cete Diuiſion.

L'Extraction de la racine quarrée.

Ou, s'il faut tirer la racine quarrée de GH, ie luy adiouſte en ligne droite FG, qui eſt l'vnité, & diuiſant FH en deux parties eſgales au point K, du centre K ie tire le cercle FIH; puis, eſleuant du point G vne ligne droite iuſques a I a angles droits ſur FH, c'eſt



* B. — C. — D. — E.

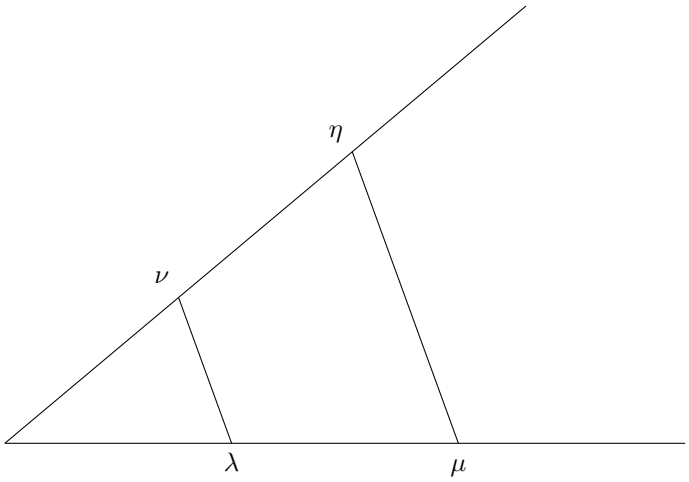
GI, la racine cherchée. Ie ne dis rien icy de la racine cubique ny des autres, a cauſe que i'en parleray plus commodement cy aprés.

Comment or peut vſer de chiffres en Geometrie.

Mais ſouuent on n'a pas beſoin de tracer ainſi ces lignes ſur le papier, & il ſuffiſt de les deſigner par quelques lettres, chaſcune par vne ſeule. Comme, pour adiouſter la ligne B D a G H, ie nomme l'vne a & l'autre b, & eſcris $a+b$; et $a-b$, pour ſouſtraire b d'a; et ab, pour les multiplier l'vne par l'autre; et $\frac{a}{b}$, pour diuiſer a par b; et aa ou a^2, pour multiplier a par ſoy meſme; et a^3, pour le multiplier encore vne fois par a, & ainſi a l'infini; et $\sqrt{a^2+b^2}$, pour tirer la racine quarrée d'a^2+b^2; et $\sqrt{\text{C.}\ a^3-b^3+abb}$, pour tirer la racine cubique d'a^3-b^3+abb, & ainſi des autres.

Où il eſt a remarquer que, par a^2 ou b^3 ou ſemblables, ie ne conçoy ordinairement que des lignes toutes ſimples, encore que, pour me ſeruir des noms vſités en l'Algebre, ie les nomme des quarrés, ou des cubes, &c.

Il eſt auſſy a remarquer que toutes les parties d'vne meſme ligne ſe doiuent ordinairement exprimer par autant de dimenſions l'vne que l'autre, lorſque l'vnité n'eſt point determinée en la queſtion : comme icy a^3 en contient autant qu'abb ou b^3, dont ſe compoſe la ligne que i'ay nommée $\sqrt{\text{C.}\ a^3-b^3+abb}$; mais que ce n'eſt pas de meſme lorſque l'vnité eſt determinée, a cauſe qu'elle peut eſtre ſouſentendue partout où il y a trop ou trop peu de dimenſions; comme, s'il faut tirer la racine cubique de $aabb-b$, il faut penſer que la quantité $aabb$ eſt diuiſée vne fois par l'vnité, & que



By similarity of triangles,

$$\frac{\eta}{\nu} = \frac{\mu}{\lambda}.$$

Thus

$$\frac{\eta}{\nu} \times \frac{\nu}{\lambda} = \frac{\mu}{\lambda} \times \frac{\nu}{\lambda}$$

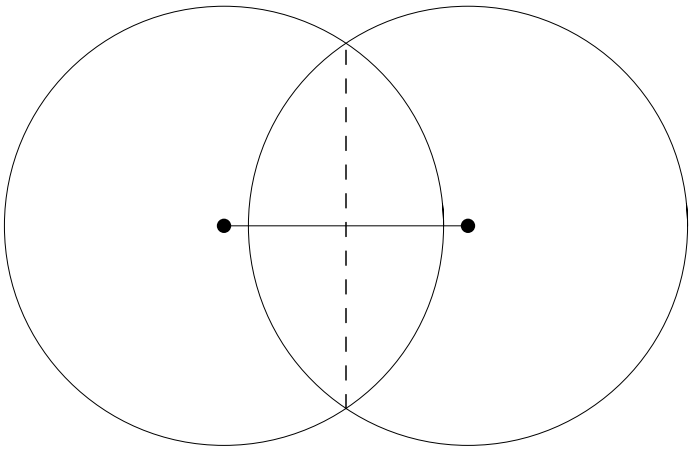
or

$$\frac{\eta}{\lambda} = \frac{\mu}{\lambda} \times \frac{\nu}{\lambda}.$$

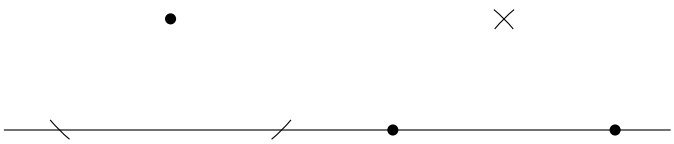
Warning

I observe that multiplication and division require that we draw a line through a point parallel to a given line. We have not given the proof that this is possible, but like the construction of the perpendicular bisector of the line joining two points, it requires taking the intersection of two circles.

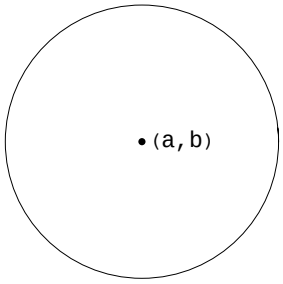
It appears therefore that we do not need to take the intersection of two circles because square roots can be constructed by intersecting a line with a circle. However, as we already noted, multiplication and division require the intersection of circles, so that the construction is by no means redundant.

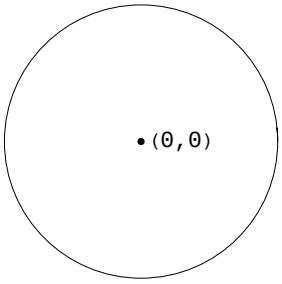


Line through a point parallel to a given line



Equations for circles in Cartesian geometry





Consider, first of all, a circle about the origin. By the Pythagorean theorem, the equation is

$$x^2 + y^2 = r^2,$$

if r is the radius of the circle and (x, y) a point on it. If we start with another circle with center (a, b), then we translate it to a circle with center at the origin.

$$(x, y) \to (x - a, y - b).$$

Since the new point is on the circle of radius 1 it satisfies

(A) $$(x - a)^2 + (y - b)^2 = r^2$$

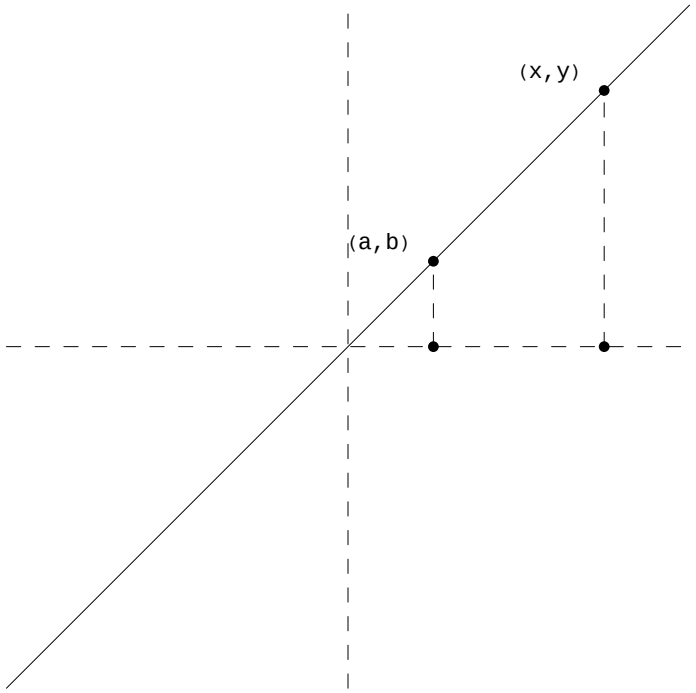
This is the equation of a general circle. If we expand all the powers it becomes

(B) $$x^2 + y^2 - 2ax - 2by + d = 0,$$

where $d = a^2 + b^2 - r^2$. Recall that for any two numbers x and a

$$(x + a)^2 = x^2 + xa + ax + a^2 = x^2 + 2ax + a^2.$$

Equations for lines in Cartesian geometry



Consider, first of all, a line through the origin. Suppose this is the line through $(0,0)$ and (a,b) and that we want to determine what equation is satisfied by a general point (x,y) on it. Since the triangle with vertices $(0,0)$, $(x,0)$ and (x,y) is similar to the triangle with vertices $(0,0)$, $(a,0)$ and (a,b) we have

$$y : b = x : a, \quad \frac{y}{b} = \frac{x}{a}, \quad ay = bx, \quad bx - ay = 0.$$

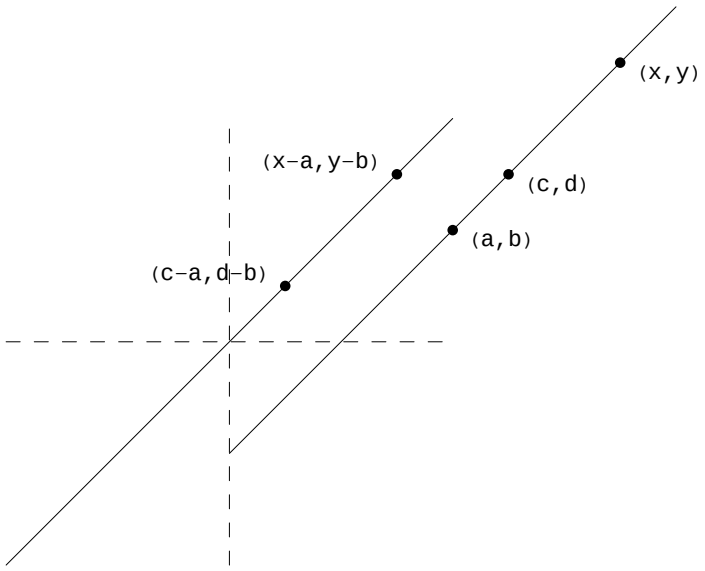
Next suppose we have an arbitrary line through the points (a,b) and (c,d) and that (x,y) is a point on it. Then translating through $(-c,-d)$ we obtain a line through the origin $(0,0)$ on which $(a-c, b-d)$ and $(x-c, y-d)$ lie. thus

$$(b-d)(x-c) - (a-c)(y-d) = 0.$$

Setting $e = (b-d)$, $f = -(a-c)$, $g = -(b-d)c + (a-c)d$ we can change this equation to

$$ex + fy + g = 0.$$

This is the general equation of a line. It contains x and y to the first power and three constants.



Observe that the coefficients e, f and g that appear in the equation of the line can be expressed algebraically in terms of the coefficients (a, b) and (c, d) of any two points on it.

Intersection of lines

In the equation for a line $ex + fy + g = 0$ that we obtained, the point $(-f, e)$ was a point on the line through the origin obtained by translation. If we started from a parallel line to obtain $e'x + f'y + g'$ then the translated line would be the same and $(-f', e')$ would lie on it. Thus by similarity of triangles,

$$e : e' = -f : -f' = f : f', \quad \frac{e}{e'} = \frac{f}{f'}, \quad ef' = fe', \quad ef' - f'e = 0.$$

The final equation is then the condition that the two equations

$$ex + fy + g = 0, \quad e'x + f'y + g' = 0$$

define parallel lines.

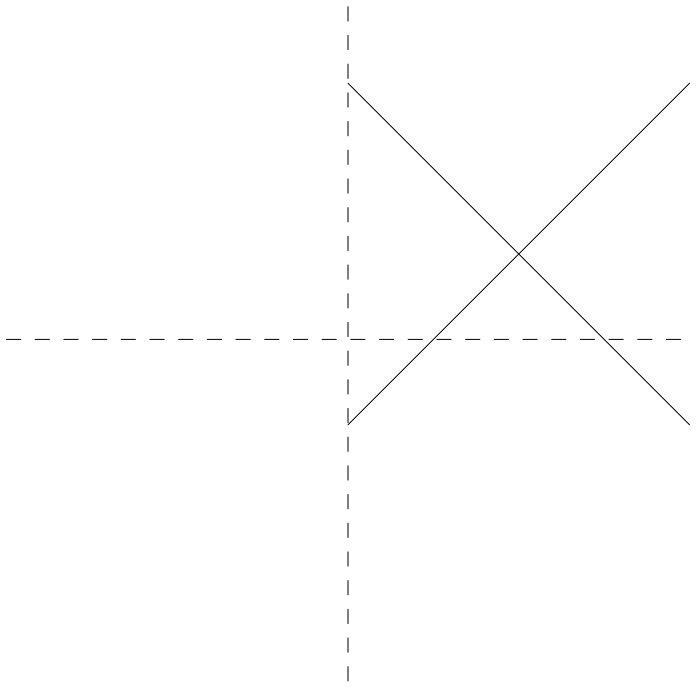
If two lines are not parallel they must have a point in common, thus a point that satisfies the two equations

$$ex + fy + g = 0,$$
$$e'x + f'y + g' = 0.$$

We solve first for x, multiplying the first equation by f' and the second by f and subtracting.

$$(f'e - fe')x + f'g - fg' = 0, \qquad x = -\frac{f'g - fg'}{f'e - e'f}.$$

Since $f'e - fe'$ is not 0, This yields x. we find y in a similar fashion. Thus from the point of view of geometrical constructions, the intersection of lines is not so interesting. It yields a point that we construct with addition, multiplication and division from the coefficients of the equations of the lines, and thus simply from the coordinates of points on the lines.

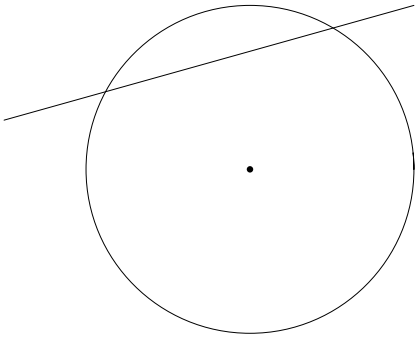


$$\begin{aligned} x - y &= 1, \\ x &= 2, \end{aligned} \qquad \begin{aligned} x + y &= 3 \\ y &= 1 \end{aligned}$$

Intersection of a line and a circle

First of all, translate the circle so that its center is at $(0, 0)$ and translate the line in the same way, so that the points of intersection are also translated. If (a, b) is the *known* center of circle, this just means subtracting a or b from the coordinates of all points. The translation can be undone at the end by adding a and b back. The circle will then have an equation

$$x^2 + y^2 = r^2.$$



Suppose the line is given by its equation

$$ax + by + c = 0, \qquad \text{New } a, b.$$

Either a or b will not be 0. I treat the case that a is not 0. Then

$$x = -\frac{by + c}{a}.$$

Thus

$$\frac{(by + c)^2}{a^2} + y^2 = r^2, \qquad (by + c)^2 + a^2y^2 = a^2r^2$$

or

$$(b^2 + a^2)y^2 + 2bcy + c^2 - a^2r^2 = 0.$$

Solve this equation by the usual formula—which then has to be simplified algebraically—to obtain

$$y = -\frac{bc}{a^2 + b^2} \pm \frac{\sqrt{b^2c^2 - (b^2 + a^2)(c^2 - a^2r^2)}}{a^2 + b^2}.$$

The conclusion is that the points of intersection can be found by calculating the square root of a number formed from known numbers: the three numbers a, b and c that are determined by two points on the line and the radius r of the circle.

An example

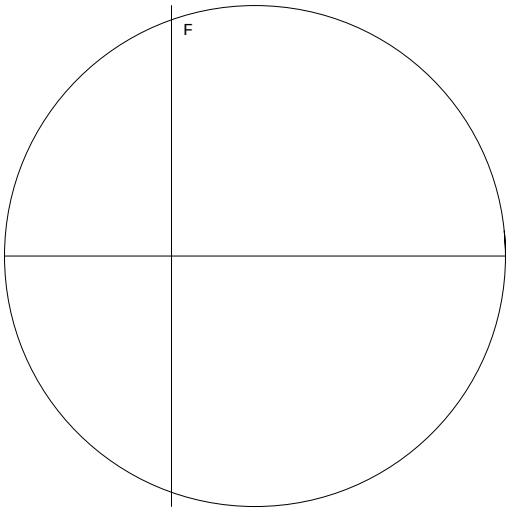
Suppose we want to find the square root of a number D. Take a circle with center at the origin and diameter $1 + D$, thus with radius $(1 + D)/2$. Take the vertical line through the point $\big((-D + 1)/2, 0\big)$. It will have an equation

$$x + \frac{D-1}{2} = 0.$$

Thus we have to substitute $a = 1$, $b = 0$, $c = (D - 1)/2$, $r = (D + 1)/2$ in the previous formula. The first term on the right is 0 and the second becomes $\sqrt{D}$ because

$$r^2 - c^2 = \frac{(D+1)^2}{4} - \frac{(D-1)^2}{4} = D.$$

Thus the second coordinate of the point on the figure is the square root of the number D, so that intersecting an appropriate line with an appropriate circle, we find the square root of any positive number. This was an observation of Descartes.



Intersection of two circles

It turns out that the intersection of two circles can also be determined by the extraction of square roots.

Once again we translate so that one of the circles has its center at the origin, or perhaps better we choose the origin to be at the center of one of the circles. Then we choose the axis of abscissas to be the line passing through the center of the two circles, and the unit distance to be the distance between the two centers. Then the first circle has an equation

$$x^2 + y^2 = r^2 \implies y^2 = r^2 - x^2$$

and the second center at $(1, 0)$

$$(x-1)^2 + y^2 = R^2 \implies (x-1)^2 + r^2 - x^2 = R^2,$$

because its center is at $(1, 0)$. Simplify to obtain

$$2x = r^2 + 1 - R^2 \implies x = \frac{r^2 + 1 - R^2}{2}$$

Thus y is equal to

$$\sqrt{r^2 - \frac{(r^2+1-R^2)^2}{4}} = \sqrt{-\frac{(r^2-R^2)^2}{4} + \frac{r^2+R^2}{2} - \frac{1}{4}}$$

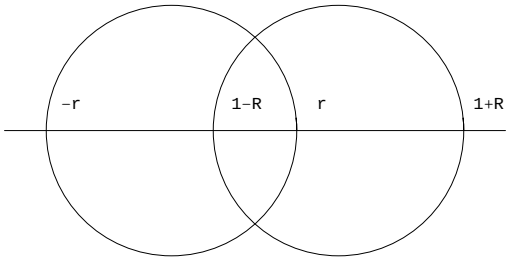
To verify this, try $r = 1/2$, $R = 1/2$, when the intersection consists of a single point with $y = 0$. As a further verification, note that if $x \geqslant 0$, thus if $r^2 + 1 \geqslant R^2$ then for y to be a real number, the expression under the square-root sign has to be positive or at least not negative, thus $r \geqslant x$ or

$$2r \geqslant r^2 + 1 - R^2 \iff R^2 \geqslant (r-1)^2.$$

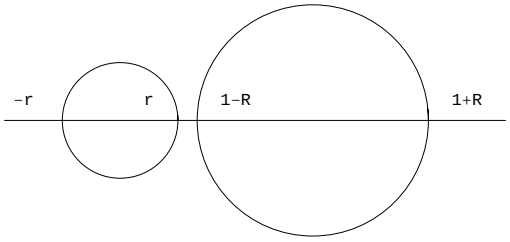
If $r \geqslant 1$ this means that $R \geqslant r - 1$ and if $r < 1$ it means that $R + r \geqslant 1$. If $x < 0$ thus if $r^2 + 1 < R^2$ then $2r$ has to be larger than or equal to $R^2 - r^2 - 1$. Thus $(r+1)^2 \geqslant R^2$ or $r + 1 > R$ which is the same as $1 - R > -r$. I give some examples.

Examples

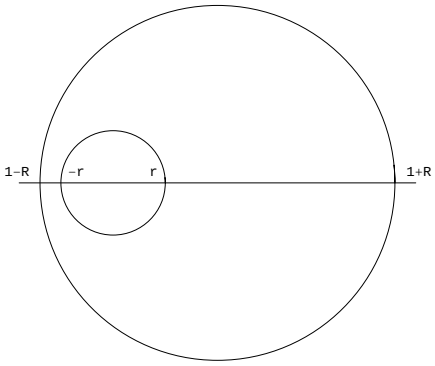
For the two circles with centers at $(0,0)$ and $(1,0)$ and radii r and R to meet the points on the axis of abscissas with abscissa $-r$, $1-R$, r, $1+R$ must lie in this order. This is illustrated in the examples.



$r = R = 0.75$



$r = 0.3, \quad R = 0.6$



$r = 0.5, \quad R = 1.7$

Some texts consulted

HEATH'S EUCLID

DESCARTES: DISCOURS DE LA METHODE

MORRIS KLINE: MATHEMATICAL THOUGHT FROM ANCIENT TO MODERN TIMES

CARL BOYER: HISTORY OF ANALYTICAL GEOMETRY

GAUSS: ARITHMETICAL INVESTIGATIONS

FELIX KLEIN: FAMOUS PROBLEMS OF ELEMENTARY GEOMETRY

On Descartes

Although it has been and remains my intention to talk about mathematics and not to allow myself any digressions, which would quickly reveal enormous gaps in my general culture, even, and perhaps especially, in that related to matters directly pertinent to mathematics and its history, I was last week questioned about the relation of Descartes's method to his mathematics and about the influence of his mathematics on that which followed. Even a brief glance at Descartes's works and his correspondence with other savants of the period renders evident that no serious answer can be offered without a knowledge of the European intellectual environment in the first decades of the seventeenth century that I do not have.

It is, however, easy to say one or two things based almost entirely on the *Discours* itself, since Descartes is quite explicit about the role of mathematics in his proposed methodology, a methodology that seems to have matured over the course of 17 years, from 1619, when he was twenty-three years old, to 1637, when he was forty-one. In the intervening years, he had seen much of the world, at least of Europe, beginning with service at the battle of the White Mountain in Bohemia, an early, decisive battle of the Thirty Years War. The last nine years before the appearance of the *Discours* were spent in the Netherlands. Although, so far as I can tell, the region was still embroiled in the aftermath of a struggle for independence and in religious conflict, Descartes's life appears to have been untroubled.

The method as such appears, according to Descartes's account, to have been formulated early. Descartes introduces its precepts with the remark that "he had studied a little when young among other parts of philosophy, logic, and among other parts of mathematics, the analysis of the geometers and algebra, three arts or sciences that seemed capable of contributing to his plan". On closer examination, logic served more to explain the known than to learn the new. As for the analysis of the ancients and the algebra of the moderns, they both seemed too abstract, and the first too constrained to the use of figures and the second to various rules and signs out of which an art had been constructed that confused the mind rather than cultivating it.

He himself proposes an art with a few simple precepts that I summarize briefly: never to accept anything as true except that which he recognizes as clearly such; to divide each difficulty that he meets into manageable pieces; to proceed in his thinking, stage by stage, from the simple to the complex; to review his thinking so carefully that he was sure that nothing had been omitted. I believe that these precepts are the essence of his method.

Then oddly enough, in spite of his previous strictures, he passes back to mathematics. I cite the text, with a more or less literal translation.

> These long chains of reasonings, all simple and easy, that geometers customarily use to arrive at their most difficult proofs, gave me occasion to imagine that everything that could be known by men, followed in the same fashion; and that provided only that one abstained from accepting anything for true that was not, and that one kept always to the necessary order in deducing one from another, there were none so abstruse that one would not ultimately arrive at them, nor so hidden that they would never be discovered. I had no difficulty in finding the correct place to begin, because I knew already that it was with the simplest and

> the easiest to know; and considering that, among all those who had already searched for the truth in the sciences, it was only the mathematicians who had been able to discover some proofs, that is to say, some certain and evident reasoning, I did not at all doubt that these would be the things they had examined; even though I hoped for no other profit than that they might accustom my wit to nourish itself with truths and not to content itself with false arguments. But I had no intention, for all that, of trying to learn all the particular sciences commonly called mathematical; and seeing that although their objects were different they nevertheless were in accord and that they did not treat of other things except for various pertinent ratios or proportions.

One might suppose that Descartes is here thinking of Book V of Euclid because the theory of proportions contained therein can be applied to lengths, areas, volumes or numbers!

> I thought that it would be more profitable to examine these proportions in general, and only in those subjects that would make a knowledge of them easier for me, but also without restricting them in any manner, in order to be able to apply them later to the other subjects for which they were appropriate. Then, having observed that to understand them I would have sometimes to consider them separately and sometimes to imagine or understand them several at a time, I thought that in order to consider them better separately, I should imagine them as lines, because I found nothing that was more simple, or that I could more distinctly represent to my imagination and my senses;

This is pertinent to the choice of problems in *La Géométrie*.

> but that in order to hold them in my mind or to understand several at once, it was necessary to explain them with some signs (ciphers), the shortest possible; and in this way I took the best from geometrical analysis and from algebra, correcting the faults of one by the other.

Of course, Descartes was by no means primarily a mathematician, and it may not be clear from these remarks that he was a mathematician at all. In fact he had two quite different mathematical talents: he was able to discover new facts, which mathematicians normally call theorems or, nowadays, results and perhaps even to prove them; and he could formulate new concepts. Of course, I cannot say with any authority how new—that would demand a knowledge of sixteenth and seventeenth century science that I do not have, but secondary sources suggest that the mathematical results of *La géométrie* are pretty much his own. The prettiest, mentioned in passing, without proof is Descartes's rule of signs, that appears, difficult as this is to believe, to have been first proved by Gauss. It would be a simple exercise for any mathematician in the room, even those to whose attention it had never been drawn. The proof that suggests itself uses differentiation and mathematical induction. I explain the statement briefly. Although it is not directly germane to our purposes, the explanation will make later concepts easier. Besides it is useful now and again, in lectures of this kind, to offer simple, comprehensible

mathematical assertions, that can be certified as genuinely elegant, if for no other reason than to give the rest of the world some feeling for what this notion means to the mathematician.

Descartes's rule of signs

> THE NUMBER OF TRUE (POSITIVE) ROOTS IS AT MOST EQUAL TO THE NUMBER OF SIGN CHANGES. THE NUMBER OF FALSE (NEGATIVE) ROOTS IS AT MOST EQUAL TO THE NUMBER OF SIGN DOUBLETS.

$$(x-1)(x-2)(x-3) = x^3 - 6x^2 + 11x - 6 = 0$$

Positive roots are: $x = 1$, 2, 3. Three sign changes; no doublets.

$$(x+1)(x+2)(x-3) = x^3 - 7x - 6 = 0$$

Positive roots are: $x = 3$. Negative: $x = -1$, -2. Two sign changes; three doublets.

$$(x+1)(x-2)(x-3) = x^3 - 4x^2 + x + 6 = 0$$

Positive roots are: $x = 2$, 3. Negative: -1. Two sign changes; one doublet.

$$(x^2+1)(x-3) = x^3 - 3x^2 + x - 3 = 0$$

Positive roots are: $x = 3$. No negative roots. Three sign changes; no doublets.

$$(x+1)(x+2)(x+3) = x^3 + 6x^2 + 11x + 6 = 0$$

No positive roots. Negative roots: -1, -2, -3. No sign changes. Three doublets.

$$(x-1)^2(x-2) = x^3 - 4x^2 + 5x - 2 = 0$$

Roots: 1, 1, 2. Three sign changes. No doublets.

NOTE: Every equation of degree n (dimension for Descartes) has exactly n roots, but they can be complex and they can be repeated!

I recall that Descartes introduction of Cartesian geometry appears in one of the three appendices to *Discours de la méthode*, the others being on optics and on rainbows. It is not yet clear to me what the relation between the *Discours* and the appendices is. The appendices are more than appendices and the body more than an introduction to the appendices.

Although the appendix on geometry is largely devoted to construction problems, they are by and large not the construction problems that concern us, thus those that can be effected with ruler and compass. Our problems are in Descartes's terminology planar problems although he sometimes referred to them as two-dimensional problems, but two-dimensional has nothing to do with the plane. Descartes simply means that in the final algebraic equation arising from the geometric problem the unknown appears as a square. He deals with these problems briefly in the first few pages and does come back to them repeatedly, but they are simply the first in a sequence of problems, followed by solid problems or problems of dimension three and four, and then by "supersolid" problems of dimension 6.

There are a number of points that he makes, that are worth recalling here. The first is that the use of ruler and compass alone is an artificial restriction. The compass is a mechanical device, as is the ruler, and other mechanical devices could be considered, of which Descartes suggests one. It constructs cube roots, fourth

roots and indeed roots of any order. The restriction to ruler and compass has, however, a great deal of historical importance, because that is what we find in Euclid, as well as great theoretical significance, because it had eventually to be asked what the algebraic and arithmetic significance of the restriction was.

Descartes wanted to play hardball. I cannot assure you that he succeeded. It would I believe take a great deal of study of earlier authors and of Descartes's contemporaries to determine exactly what his contributions were.

Since he wanted to demonstrate that the use of algebraic equations and coordinates permitted the discovery and demonstration of new theorems, most of the appendix is devoted to indeterminate construction problems, thus to problems that define a curve, or to problems that require more than a ruler and compass for their solution.

The free passage back and forth from the geometry to the algebra, allows him to convert one kind of geometric problem to another. For example to duplicate a cube, one needs to extract the cube root of 2. If the side of a cube is a, so that its volume is a^3 then a cube of side $\sqrt[3]{2}a$ has double its volume, namely $2a$. Descartes showed that all cubic equations, in particular

$$x^3 = 2$$

could be solved by intersecting circles with a conic section, in particular with a parabola. Indeed he shows that all cubic and quartic equations can be solved geometrically in this way.

In other words, cubic and quartic irrationalities are all constructed by intersecting circles and parabolas. The converse is also true.

Eventually he reaches irrationalities of degree, or as he says dimension, 5 and 6, but here the construction of solutions requires the use of more complicated mechanical devices, requiring moving parabolas.

There is among Descartes's often Delphic remarks one that, to me at least, anticipates in a curious way the use of complex numbers. He observes, for example, that the geometric construction of the solutions of cubic equations entails being able to perform exactly two constructions, that of the cube root of a positive number, thus of constructing two mean proportionals to two given lengths, and trisection of an arbitrary angle. We will come back to this remark later, but neither exactly what Descartes had in mind nor what he had learned from others is clear to me.

If

$$YA : YB = YB : YC = YC : YD$$

then

$$\left(\frac{YA}{YB}\right)^3 = \frac{YA}{YB}\frac{YB}{YC}\frac{YC}{YD} = \frac{YA}{YD}$$

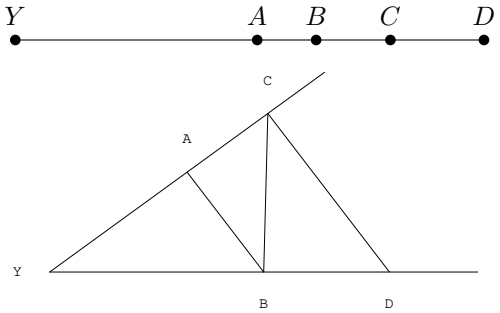
The first relations are referred to by saying that YB and YC are two mean proportionals between YA and YD. If $YA : YD = 1 : 2$ then in effect we want

$$\left(\frac{YA}{YB}\right)^3 = \frac{1}{2}$$

or

$$\left(\frac{YB}{YA}\right)^3 = 2$$

Thus if YA is the side of a cube then YB will be the side of a cube of twice the volume.



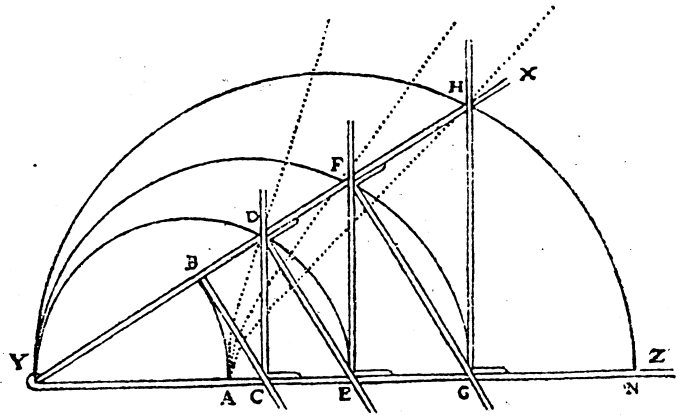
In the same way one can ask for four mean proportionals,

$$YA : YB = YB : YC = YC : YD = YD : YE = YE : YF$$

which implies that

$$\left(\frac{YA}{YB}\right)^5 = \frac{YA}{YF}$$

Voyés les lignes AB, AD, AF & ſemblables, que ie ſuppoſe auoir eſté deſcrites par l'ayde de l'inſtrument YZ[a], qui eſt compoſé de pluſieurs reigles, tellement iointes que, celle qui eſt marquée YZ eſtant areſtée ſur la ligne AN, on peut ouurir & fermer l'angle XYZ, & que, lorſqu'il eſt tout fermé, les poins B, C, D, <E>[b] F, G, H ſont tous aſſemblés au point A;



mais qu'a meſure qu'on l'ouure, la reigle BC, qui eſt iointe a angles droits auec XY au point B, pouſſe vers Z la reigle CD, qui coule ſur YZ en faiſant touſiours des angles droits auec elle; & CD pouſſe DE, qui coule tout de meſme ſur YX en demeurant parallele a BC; DE pouſſe EF; EF pouſſe FG; celle cy pouſſe GH; & on en peut conceuoir vne infinité d'autres, qui ſe pouſſent conſequutiuement en meſme façon, & dont les vnes facent touſiours les meſmes angles auec YX, & les autres auec YZ. Or, pendant

a. XYZ *Schooten.*
b. E *a été ajouté par Schooten.*

ſi la quantité inconnuë n'a que trois dimenſions; ou bien a telle :

$$\zeta^4 \propto \star \cdot ap\zeta\zeta \cdot aaq\zeta \cdot a^3 r,$$

ſi elle en a quatre; ou bien, en prenant a pour l'vnité,

a telle : $\zeta^3 \propto \star \cdot p\zeta \cdot q$

& a telle : $\zeta^4 \propto \star \cdot p\zeta\zeta \cdot q\zeta \cdot r$ (*).

Aprés cela, ſuppoſant que la Parabole FAG eſt deſia deſcrite, & que ſon aiſſieu eſt ACDKL, & que ſon coſté droit eſt a ou 1 (*), dont AC eſt la moitié, & enfin que le point C eſt au dedans de cete Parabole, & que A en eſt le ſommet : il faut faire $CD \propto \frac{1}{2}p$, & la prendre du meſme coſté qu'eſt le point A au regard du point C[a], s'il y a $+p$ en l'Equation; mais, s'il y a $-p$, il faut la prendre de l'autre coſté. Et du point D, ou bien, ſi la quantité p eſtoit nulle, du point C, il faut eſleuer vne ligne a angles droits iuſques a E, en ſorte qu'elle ſoit eſgale a $\frac{1}{2}q$. Et enfin,

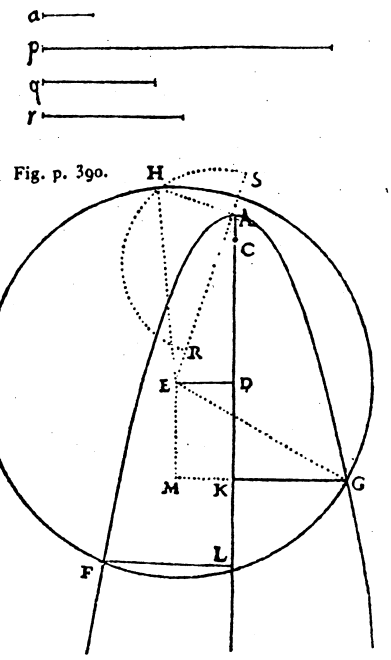


Fig. p. 390.

(*) T. — V.

a. Lire « qu'est le point C au regard du point A ».

du centre E, il faut deſcrire le cercle FG, dont le demi-diametre ſoit AE, ſi l'Equation n'eſt que cubique, en ſorte que la quantité r ſoit nulle. Mais quand il y a $+r$, il faut, dans cete ligne AE prolongée, prendre d'vn coſté AR eſgale a r, & de l'autre AS eſgale au coſté droit de la Parabole, qui eſt 1 ; & ayant deſcrit vn cercle dont le diametre ſoit RS, il faut faire AH perpendiculaire ſur AE, laquelle AH rencontre ce cercle RHS au point H, qui eſt celuy par où l'autre cercle FHG doit paſſer. Et quand il y

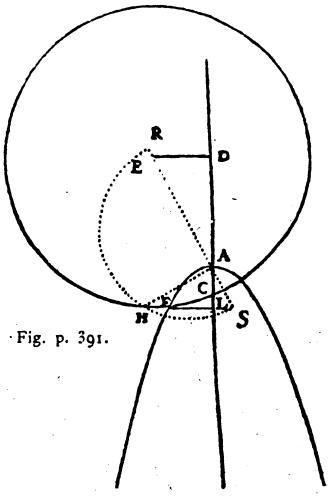
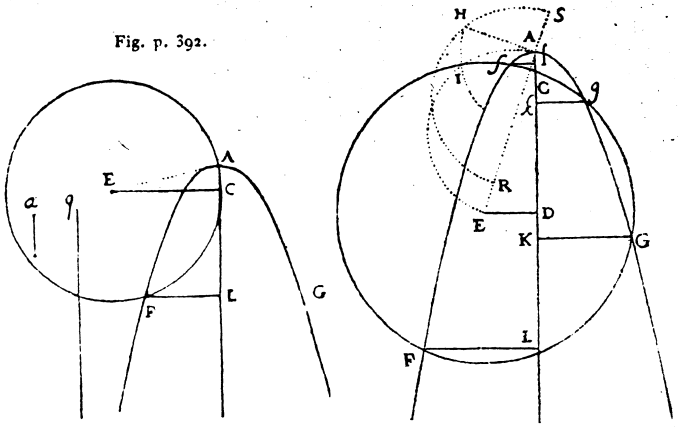


Fig. p. 391.

Fig. p. 392.



$a - r$, il faut, aprés auoir ainſi trouué la ligne AH,

Conclusion

If a geometric construction requires in its analytic form nothing but addition, subtraction, multiplication, division, and the extraction of square roots, then it can be achieved with ruler and compass. These arithmetic operations are to be applied to the two coordinates of each point given by the construction problem. Conversely if it can be achieved with ruler and compass, then when represented analytically all points involved in the construction will have coordinates that can be obtained from those of the points initially given by these five arithmetic operations. The results may be very complicated. If (a, b) and (c, d) are two of the points given, one new coordinate might be

$$\sqrt{a^2 + \frac{ac^2}{\sqrt{b^2 + d^2}}} - \sqrt{7b^2 + c\sqrt{a^2 + \frac{2b^4}{\sqrt{c^2 + d^2}}}}$$

This point reached, we can now concentrate almost entirely on the algebra!

Complex numbers

We want to analyze in an algebraic manner, thus in terms of Cartesian geometry, the geometric construction of the regular pentagon. For this it is best to go beyond Descartes and to employ *complex* numbers. I begin with a rapid review of their definition.

Recall that the formula for the solution of a quadratic equation

$$ax^2 + bx + c = 0$$

is

$$x = -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a} \tag{I}$$

Thus there are two solutions, different save in the exceptional case that $b^2 = 4ac$. If $b^2 - 4ac$ is negative, the square root does not exist in the usual sense and we are, in order to have a complete theory, forced to introduce purely formally the square roots of negative numbers. If C is positive,

$$\sqrt{-C} = \sqrt{-1}\sqrt{C}, \tag{II}$$

so that once we have a square root of -1 that we are prepared to multiply with any *real* number we have the square root of any number. If we are prepared to add formally a real number to one of these purely imaginary numbers, in which we permit both the positive square root of C and the negative square root, then we have all the numbers

$$A + \sqrt{-1}B = A + B\sqrt{-1}$$

that appear in (I), so that we can formally solve any quadratic equation. If $b^2 - 4ac < 0$, take

$$A = -\frac{b}{2a}, \quad B = \sqrt{4ac - b^2}$$

The algebra of complex numbers

We need to be able to perform the usual arithmetic operations on complex numbers. Rather than constantly writing $\sqrt{-1}$, it is the mathematician's habit to write simply i. Thus i is a number whose square is -1 and the only trick in operating with i or with the square root of -1 is to replace i^2 with -1 whenever it occurs. Thus

$$(a+bi)\times(c+di) = ac + adi + bci + bdi^2 = (ac-bd) + (ad+bc)i$$

More generally when adding, subtracting, and multiplying in any order any number of complex numbers the result is always expressed finally as the sum of a real number a and another real number b times i.

We add two complex numbers

$$(a+bi)+(c+di) = (a+c)+(b+d)i.$$

Subtraction is the same.

Division is more difficult. Suppose $A = a+bi$ and $C = c+di$ are two complex numbers, the second of which is not $0 = 0+0i$ and we want to solve

$$\frac{A}{C} = E \Longleftrightarrow A = CE.$$

Write E out explicitly $E = e+fi$. Then

$$(a+bi) = (c+di)\times(e+fi).$$

Multiply both sides by $c-di$. Since

$$(c-di)\times(c+di) = c^2+d^2,$$

we have

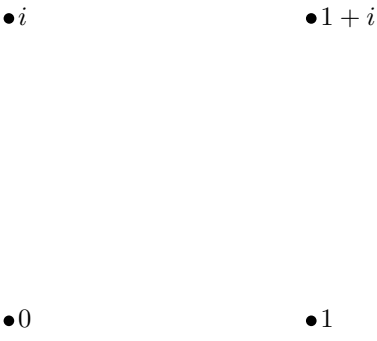
$$(a+bi)\times(c-di) = (c^2+d^2)\times(e+fi)$$

or

$$e+fi = (a+bi)\times\left(\frac{c}{c^2+d^2} - \frac{d}{c^2+d^2}i\right).$$

Complex numbers and Cartesian geometry

We usually think of complex numbers as being points in the Cartesian plane, the complex number $a+bi$ being associated, or even identified in our thinking, with the point (a,b).



Division continued

The formula for division can be written as

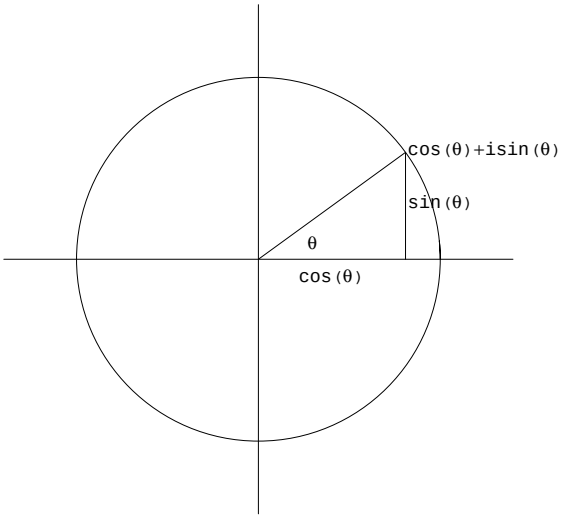
$$\frac{1}{c+di} = \frac{c}{c^2+d^2} - \frac{d}{c^2+d^2}i.$$

Observe also in passing that

$$(c+di)\times(c-di) = c^2+d^2.$$

This is a positive number that is 0 only if the complex number is 0.

Complex numbers on the unit circle and rotation



Multiply $x+yi$ by $\cos(\theta)+i\sin(\theta)$:

$$\big(\cos(\theta)+i\sin(\theta)\big)\times(x+iy) = \big(\cos(\theta)x-\sin(\theta)y\big)+i\big(\sin(\theta)x+\cos(\theta)y\big).$$

According to an earlier formula the effect is to rotate the point (x,y) through an angle θ. In particular,

$$\big(\cos(\theta)+i\sin(\theta)\big)\big(\cos(\varphi)+i\sin(\varphi)\big) = \big(\cos(\theta+\varphi)+i\sin(\theta+\varphi)\big).$$

Taking $\varphi=\theta$ we obtain

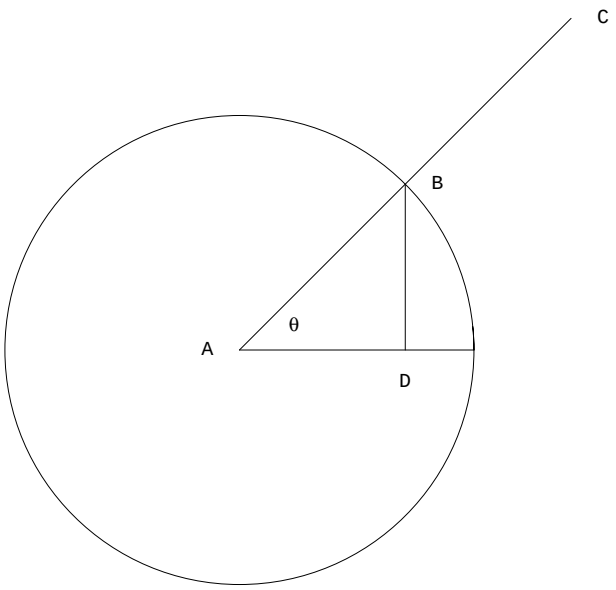
$$\big(\cos(\theta)+i\sin(\theta)\big)^2 = \cos(2\theta)+i\sin(2\theta),$$

and

$$\big(\cos(\theta/2)+i\sin(\theta/2)\big)^2 = \cos(\theta)+i\sin(\theta).$$

Lecture 6

Square roots of complex numbers



$$C = (x, y) \qquad B = \big(\cos(\theta), \sin(\theta)\big)$$
$$AC = \sqrt{x^2 + y^2} = r \qquad AB = 1$$
$$(x, y) = \big(r\cos(\theta), r\sin(\theta)\big), \qquad x + iy = r \times \big(\cos(\theta) + i\sin(\theta)\big)$$
$$\sqrt{x + iy} = \sqrt{r}\sqrt{\cos(\theta) + i\sin(\theta)} = \sqrt{r}\big(\cos(\theta/2) + i\sin(\theta/2)\big)$$

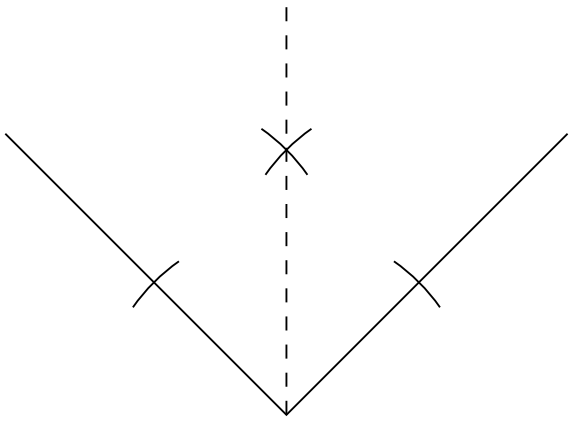
We know that $\sqrt{r}$ can be found with ruler and compass. So can

$$\sqrt{\cos(\theta) + i\sin(\theta)}$$

because it is simply a matter of bisecting the angle θ.

Date of lecture: Fall term, November 30, 1999.

Bisection of an angle



Other roots of complex numbers

Cube roots.

$$\begin{aligned}\big(\cos(\theta)+i\sin(\theta)\big)^3 &= \big(\cos(\theta)+i\sin(\theta)\big)\big(\cos(\theta)+i\sin(\theta)\big)^2 \\ &= \big(\cos(\theta)+i\sin(\theta)\big)\big(\cos(2\theta)+i\sin(2\theta)\big) \\ &= \cos(3\theta)+i\sin(3\theta)\end{aligned} \tag{I}$$

Thus

$$\big(\cos(\theta/3)+i\sin(\theta/3)\big)^3 = \cos(\theta)+i\sin(\theta) \tag{II}$$

and

$$\sqrt[3]{\cos(\theta)+i\sin(\theta)} = \cos(\theta/3)+i\sin(\theta/3) \tag{III}$$

We apply equation (I) to $\theta = 0$, $\theta = 2\pi/3$ or $\theta = 4\pi/3$. Then 3θ is 0, 2π or 4π so that

$$\cos(3\theta)+i\sin(3\theta) = 1 + 0\cdot i = 1.$$

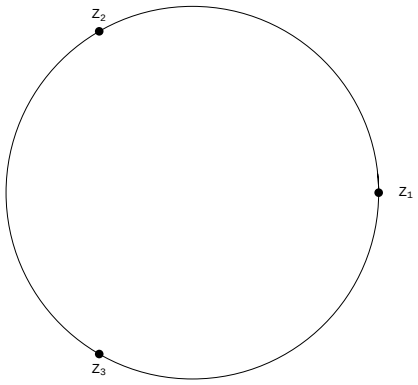
So we have found three cube roots of 1. There are no more! The first is

$$\cos(0)+i\sin(0) = 1,$$

hardly a surprise. In order to display these three points graphically, we denote them

$$Z_1 = 1, \quad Z_2 = \cos(2\pi/3)+i\sin(2\pi/3), \quad Z_3 = \cos(4\pi/3)+i\sin(4\pi/3).$$

Cube roots continued



These three complex numbers satisfy the equation

$$z^3 - 1 = 0.$$

We divide $z^3 - 1$ by $z - 1$. We use long division.

(1) First step.

$$\begin{array}{ll} z^3 - 1 & \\ \dfrac{z^3 - z^2}{z^2 - 1} & \qquad z^2 \times (z-1) \end{array}$$

(2) Second step.

$$\begin{array}{ll} z^2-1 & \\ \hline z^2-z^1 & z\times(z-1) \\ z^1-1 & \end{array}$$

(3) Third step.

$$\begin{array}{ll} z^1-1 & \\ \hline z^1-1 & 1\times(z-1) \\ 0 & \end{array}$$

Thus the remainder is 0 and

$$\frac{z^3-1}{z-1}=z^2+z+1$$

or

$$z^3-1=(z-1)(z^2+z+1)$$

Substitute z_2. Then

$$0=(z_2-1)(z_2^2+z_2+1) \implies z_2^2+z_2+1=0.$$

We solve this equation.

$$z_2=-\frac{1}{2}\pm\frac{\sqrt{-3}}{2}=-\frac{1}{2}\pm i\frac{\sqrt{3}}{2}.$$

Thus

$$z_2=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$$

so that $\cos(2\pi/3)=1/2$, $\sin(2\pi/3)=\sqrt{3}/2$. For similar reasons z_3 is the other root:

$$z_3=-\frac{1}{2}-i\frac{\sqrt{3}}{2}.$$

One more example of long division

To divide $2z^3+3z^2+4z+1$ by z^2+3z+2,

(1) First step:

$$\begin{array}{ll} 2z^3+3z^2+4z+1 & \\ \hline 2z^3+6z^2+4z & 2z\times(z^2+3z+2) \\ -3z^2+1 & \end{array}$$

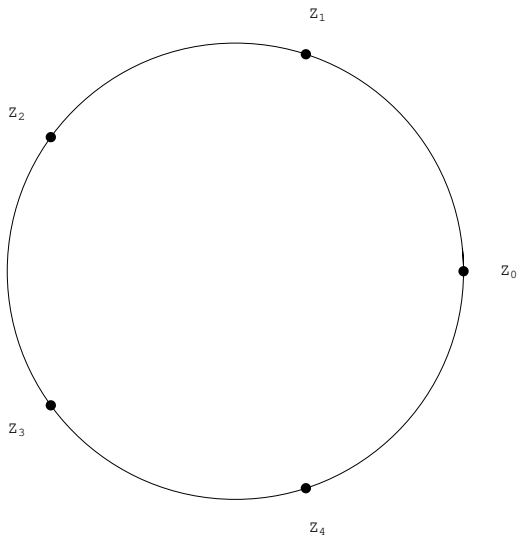
(2) Second step:

$$\begin{array}{ll} -3z^2+1 & \\ \hline -3z^2-9z-6 & -3\times(z^2+3z+2) \\ 9z+7 & \end{array}$$

We have divided by a polynomial of degree two and the remainder has smaller degree, namely one. The result is:

$$2z^3+3z^2+4z+1=(2z-3)\times(z^2+3z+2)+9z+7$$

Fifth roots of unity



After the discussion of the cube roots of unity, it should come as no surprise that the fifth roots of unity are the numbers

$$\cos(2k\pi/5) + i\sin(2k\pi/5), \qquad k = 0, 1, 2, 3, 4.$$

They form the vertices of a regular pentagon. Thus if we can show that they can be obtained by repeatedly extracting square roots, we will have an algebraic proof of the possibility of constructing the regular pentagon with ruler and compass.

Algebraic symmetries I

Just as we can factor

$$z^3 - 1 = (z - 1)(z^2 + z + 1),$$

we can factor

$$z^5 - 1 = (z - 1)(z^4 + z^3 + z^2 + z + 1).$$

It follows that each of the four numbers

$$z_i = \cos(2k\pi/5) + i\sin(2k\pi/5), \qquad k = 1, 2, 3, 4$$

satisfies the equation

$$z^4 + z^3 + z^2 + z + 1 = 0.$$

Thus our algebraic interpretation of the five vertices of the regular pentagon as the five fifth roots of unity has destroyed the five-fold symmetry. We have distinguished one vertex, placing it at the point 1=1+0i. So we now have to look for a different kind of symmetry, that among the four remaining vertices, or better the four remaining roots.

There is a one obvious symmetry, that which interchanges z_1 and z_4 as well as z_2 and z_3. This is an *algebraic* as well as a *geometric* symmetry because it is just a matter of replacing each of the numbers by its complex conjugate

$$a + bi \to a - bi$$

and

$$(a+bi)\times(c+di) = ac-bd+(ad+bc)i \to ac-bd-(ad+bc)i = (a-bi)\times(c-di)$$

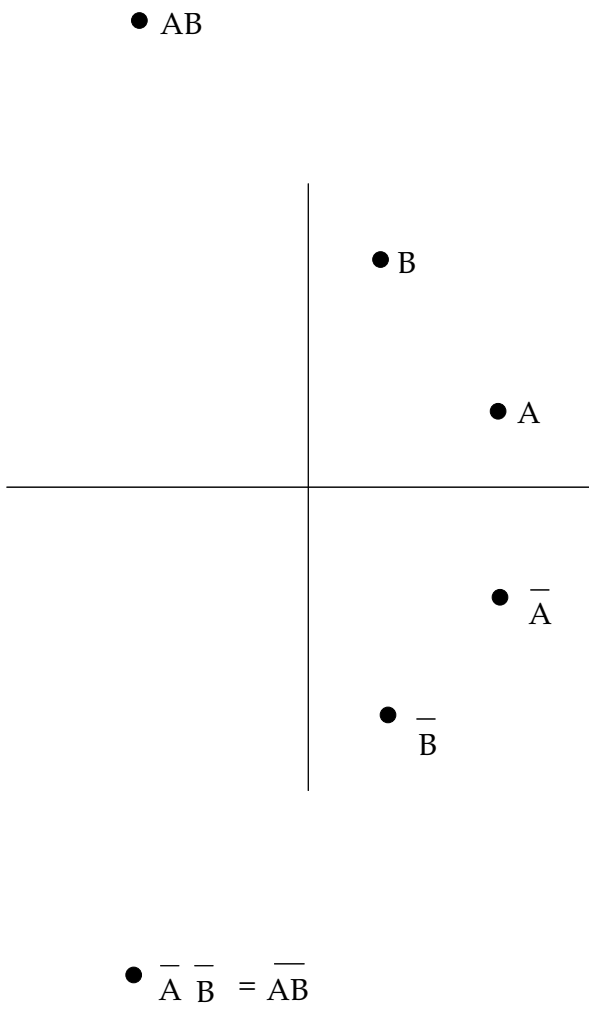
I take it as obvious that the complex conjugate of the sum or the difference of two complex numbers is the sum or the difference of their complex conjugates.

$$(a+bi)+(c+di) = (a+c)+(b+d)i \to (a+bi)-(c+d)i = (a-bi)+(c-di)$$

In other words the operation of complex conjugation that interchanges z_1 and z_4 as well as z_2 and z_3

$$z_1 \leftrightarrow z_4, \quad z_2 \leftrightarrow z_3$$

is like reflection in a mirror. All *arithmetic* properties are faithfully preserved.


AB
B
A
$\overline{A}$
$\overline{B}$
$\overline{A}\ \overline{B} = \overline{AB}$

Small remarks

It is sometimes useful to recall that the relation

$$z_1^4 + z_1^3 + z_1^2 + z_1 + 1 = 0$$

is the same as

$$z_4 + z_3 + z_2 + z_1 + z_0 = 0$$

Why is, for example, $z_1 z_2 = z_3$?

$$\big(\cos(\theta) + i\sin(\theta)\big)\big(\cos(\varphi) + i\sin(\varphi)\big) = \cos(\theta + \varphi) + i\sin(\theta + \varphi).$$

Take $\theta = 2\pi/5$ and $\varphi = 4\pi/5$. Then $\theta + \varphi = 6\pi/5$. This becomes

$$z_1 z_2 = z_3.$$

One shows in the same way that, for example, $z_2 z_2 = z_4$. Observe also that, along the same lines,

$$z_1^7 = \big(\cos(2\pi/5) + i\sin(2\pi/5)\big)^7 = \cos(14\pi/5) + i\sin(14\pi/5)$$

and

$$\cos(14\pi/5) + i\sin(14\pi/5) = \cos(4\pi/5) + i\sin(4\pi/5) = z_2$$

This is because the angle $14\pi/5$ is equal to $2\pi + 4\pi/5$ and the cosine and sine do not change when 2π is added to or subtracted from an angle. Indeed, in some respects, the angle itself does not change! (Note: this statement is correct, but calls for some reflection!)

Algebraic symmetries II

This is because i is just a symbol that stands for the square root of -1 and $-i$ is then introduced and defined by the condition that

$$i + (-i) = 0.$$

But $-i$ is also just a symbol and can be taken as the primary symbol.[1] Then i is a second symbol that functions as $-(-i)$. Even if i is taken to have some meaning beyond that of a mere symbol, it cannot have a different meaning than $-i$, so that the two have to be regarded as perfectly interchangeable.

Are there other symmetries of this kind?

Whether there are other symmetries of this kind affecting all complex numbers is not a question for us, but we can ask whether there are symmetries of this kind affecting just z_1, z_2, z_3 and z_4. Before we do, we make use of the symmetry at hand. Since $z_1 z_1 = z_2$, $z_1 z_2 = z_3$, $z_1 z_3 = z_4$, $z_1 z_4 = 1$, $z_2 z_2 = z_4$, $z_2 z_3 = 1$ and so on, and since in addition

$$1 = -z_1 - z_2 - z_3 - z_4$$

the numbers

$$az_1 + bz_2 + cz_3 + dz_4,$$

where a, b, c and d are arbitrary ordinary fractions form a collection closed under addition, subtraction, multiplication, and even as it turns out division. The numbers that are equal to their own reflections can be singled out. These are the numbers

$$a(z_1 + z_4) + b(z_2 + z_3).$$

[1] The distinguishing characteristic of i is that $i^2 = -1$ but this characteristic is shared by $-i$.

The appearance of $\sqrt{5}$

Let w be the number $z_1 + z_4$. It is equal to its own reflection. So is its square. Thus

$$w^2 = a(z_1 + z_4) + b(z_2 + z_3) = (a-b)(z_1 + z_4) + b(z_1 + z_2 + z_3 + z_4) = (a-b)w - b.$$

Thus w satisfies a quadratic equation

$$w^2 + cw + d = 0, \qquad c = b - a, \quad d = b.$$

We calculate this equation

$$w^2 = (z_1 + z_4)^2 = z_1^2 + z_1 z_4 + z_4 z_1 + z_4^2 = z_2 + 1 + 1 + z_3 = 2 - 1 - z_1 - z_4 = 1 - w.$$

Thus

$$w^2 + w - 1 = 0 \qquad w = \frac{-1 \pm \sqrt{1+4}}{2}.$$

Since w is a positive number,

$$w = \frac{-1 + \sqrt{5}}{2}.$$

In other words, w can as we know be constructed with ruler and compass. Since

$$z_1 + z_4 = w \iff z_1 + \frac{1}{z_1} = w \iff z_1^2 + 1 = z_1 w$$

we have

$$z_1 = \frac{w \pm \sqrt{w^2 - 4}}{2}.$$

Since $w^2 = 1 - w$, this is

$$\frac{w \pm \sqrt{-3 - w}}{2} = \frac{-1 + \sqrt{5}}{4} \pm \frac{\sqrt{-\frac{5}{2} - \frac{\sqrt{5}}{2}}}{2}.$$

Since z_1 lies above the axis of abscissas,

$$z_1 = \frac{-1 + \sqrt{5}}{4} + i\frac{\sqrt{\frac{5+\sqrt{5}}{2}}}{2}.$$

Symmetries III

Having found z_1, we can easily find z_4, its complex conjugate, and we can certainly find z_2 by squaring z_1. We can also find z_2 by working with $z_2 + z_3$ rather than w. This is, however, straightforward algebra. As Descartes insisted, the algebra often turns a problem into an almost unthinking manipulation of symbols, a turn that it can indeed often take, but we prefer another direction. This is the direction taken by Gauss.

Let ζ be the number z_1. Then $z_2 = \zeta^2$, $z_3 = \zeta^3$, and $z_4 = \zeta^4 = -1 - \zeta - \zeta^2 - \zeta^3$ because

$$\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0 \tag{I}$$

Our numbers $ez_1 + fz_2 + gz_3 + hz_4$ can also be expressed as

$$a + b\zeta + c\zeta^2 + d\zeta^3$$

$$a = -h, \quad b = e - h, \quad c = f - h, \quad d = g - h.$$

Are these numbers all different?

This is an important question! The answer is yes and I shall give a proof following Gauss. We first note the consequences. Since the numbers are all different, we cannot have an equation

$$a + b\zeta + c\zeta^2 + d\zeta^3 = 0 = 0 + 0\zeta + 0\zeta^2 + 0\zeta^3$$

unless $a = b = c = d = 0$. This means that ζ satisfies the equation

$$Z^4 + Z^3 + Z^2 + Z + 1 = 0 \tag{I}$$

and essentially only this equation, because if we have any other such as

$$Z^6 + AZ^5 + BZ^4 + CZ^3 + DZ^2 + EZ + F = 0 \tag{II}$$

then by the process of long division we will have

$$Z^6 + AZ^5 + BZ^4 + CZ^3 + DZ^2 + EZ + F = (Z^2 + GZ + H)(Z^4 + Z^3 + Z^2 + Z + 1) + PZ^3 + QZ^2 + RZ + S$$

so that

$$P\zeta^3 + Q\zeta^2 + R\zeta + S = 0$$

We have just seen that this implies $P = Q = R = S = 0$. Thus

$$Z^6 + AZ^5 + BZ^4 + CZ^3 + DZ^2 + EZ + F = (Z^2 + GZ + H) \times (Z^4 + Z^3 + Z^2 + Z + 1)$$

and (II) is a consequence of (I).

Symmetries IV

This means that, from an abstract point of view, ζ is simply a number that satisfies the equation

$$\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$$

and no other. But z_2, z_3 and z_4 have exactly the same property. Thus *for strictly algebraic purposes* we could take ζ to be z_2 rather than z_1. Thus z_1 is replaced by z_2. Since *all* algebraic relations are to be preserved, this entails replacing $z_2 = z_1^2$ by $z_2^2 = z_1^4 = z_4$ and $z_3 = z_1^3$ by $z_2^3 = z_1^6 = z_1$. Once again, because all algebraic relations are to be respected, the number

$$z_4 = z_1^4 = -1 - z_1 - z_1^2 - z_1^3$$

is to be replaced by

$$-1 - z_2 - z_2^2 - z_3^3 = z_2^4 = z_1^8 = z_1^3 = z_3.$$

In general a number

$$a + b\zeta + c\zeta^2 + d\zeta^3 = a + bz_1 + cz_1^2 + dz_1^3 = (b - a)z_1 + (c - a)z_2 + (d - a)z_3 - az_4$$

is replaced by

$$a + bz_2 + cz_2^2 + dz_2^3 = a + bz_1^2 + cz_1^4 + dz_1 = (a - c) + (d - c)z_1 + (b - c)z_1^2 - cz_1^3$$

which is a number of the same kind. For example

$$z_3 = z_1^3 \to z_1 \qquad z_4 = z_1^4 \to z_2^4 = z_1^8 = z_1^3 = z_3.$$

Forms of algebraic symmetries

The symmetry just examined can be viewed in two ways:

1) It takes the sequence $\{z_1, z_2, z_3, z_4\}$ of all roots of

$$Z^4 + Z^3 + Z^2 + Z + 1$$

to a sequence formed from the same numbers but in a different order

$$\{z_2, z_4, z_1, z_3\}.$$

2) It takes any number

(I) $$az_1 + bz_2 + cz_3 + dz_4$$

to a number

(II) $$az_2 + bz_4 + cz_1 + dz_3$$

of the same kind.

This is the kind of symmetry that was later investigated in general by Galois. We have to spend some time growing accustomed to it. Suppose we apply the symmetry twice. Then

$$z_1 \to z_2 \to z_4$$
$$z_2 \to z_4 \to z_3$$
$$z_3 \to z_1 \to z_2$$
$$z_4 \to z_3 \to z_1$$

Thus applying the basic symmetry twice leads to the first symmetry considered, complex conjugation. We apply it again.

$$z_1 \to z_4 \to z_3$$
$$z_2 \to z_3 \to z_1$$
$$z_3 \to z_2 \to z_4$$
$$z_4 \to z_1 \to z_2$$

Yet again!

$$z_1 \to z_3 \to z_1$$
$$z_2 \to z_1 \to z_2$$
$$z_3 \to z_4 \to z_3$$
$$z_4 \to z_2 \to z_4$$

So the symmetry when repeated four times comes back where it began. It is a four-fold symmetry.

Anticipating Galois and his successors

No matter which of the numbers z_1, z_2, z_3, z_4 we take ζ to be, the collection of numbers

$$a + b\zeta + c\zeta^3 + d\zeta^4, \qquad a,\ b,\ c,\ d \text{ all fractions} \tag{I}$$

is the same. Modern mathematicians usually call the collection a field. The sum and the product of two numbers of this sort are again numbers of the same sort. This we have seen already. I give another example.

$$(1+\zeta)(1+\zeta^3) = 1 + \zeta + \zeta^3 + \zeta^4 = -\zeta^2.$$

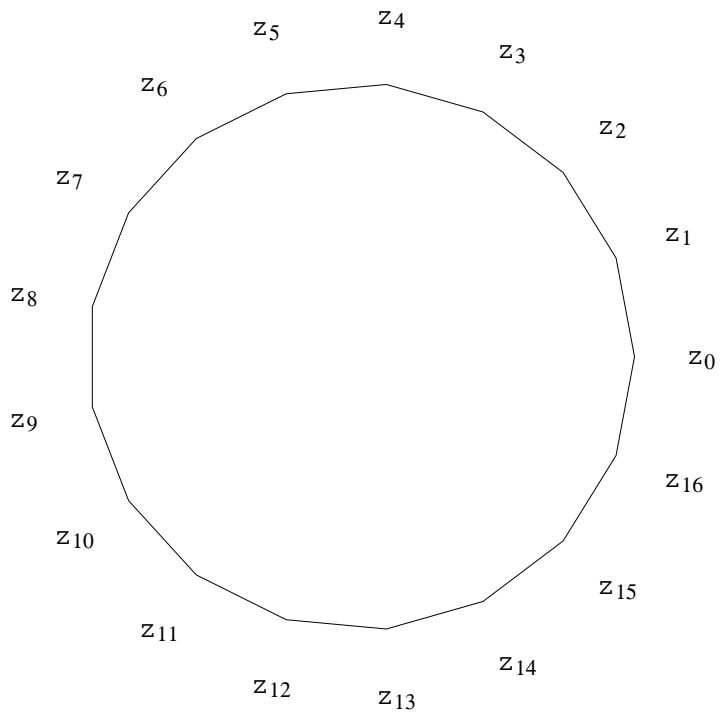
Any symmetry of this collection that respect the algebraic operations will take 0 to 0 and 1 to 1. Then adding and dividing it takes any fraction a/b to a/b. Moreover any root of

$$Z^4 + Z^3 + Z^2 + Z + 1 = 0$$

will be taken to another root. Thus z_1 will be taken to z_1, z_2, z_3 or z_4. In other words, the symmetry will be one of the four (including the trivial symmetry!) we already have. Denote the one taking z_1 to z_2 by the letter σ. Then repeating σ to obtain $\sigma\sigma = \sigma^2$ we obtain the symmetry taking z_1 to z_4. Repeating again, we obtain $\sigma\sigma\sigma = \sigma^3$ which takes z_1 to z_3. Repeating again, we find that $\sigma\sigma\sigma\sigma = \sigma^4$ is the trivial symmetry.

Inside the collection of numbers there is a smaller collection of numbers that have a special symmetry. We met them before. They are those that are not affected by σ^2, thus by complex conjugation. They are the numbers $a + bw$, $w = z_1 + z_4$. We were able to construct z_1 by successive square roots, by first singling out this special collection of numbers, finding that any number in it satisfied a quadratic equation with fractions as coefficients, in particular that $w^2 + w - 1 = 0$, so that $w = \frac{(-1+\sqrt{5})}{2}$, and then solving $z_1^2 - z_1 w + 1 = 0$. We now apply these ideas, which I hope are clear, to the heptadecagon!

The Heptadecagon



$$z_k = \cos(2k\pi/17) + i\sin(2k\pi/17)$$

From the *Disquisitiones Arithmeticae*

There is a famous remark from the introduction to the seventh and last chapter of the *Disquisitiones* that I quote here. What it anticipates is the study of the division points on elliptic curves, in the remark a special elliptic curve, a study that led over the course of the nineteenth and twentieth century to many things, especially complex multiplication and ℓ-adic representations, that are relevant to the Shimura-Taniyama-Weil conjecture,

> *Ceterum principia theoriae, quam exponere aggredimur, multo latius patent, quam hic extenduntur. Namque non solum ad functiones circulares, sed pari successu ad multas alias functiones transscendentes applicari possunt, e.g. ad eas, quae ab integrali*
>
> $$\int \frac{dx}{\sqrt{1-x^4}}$$
>
> *pendent, praetereaque etiam ad variam congruentarium genera: sed quoniam de illis functionibus transscendentibus amplum opus peculiare paramus, de congruentiis autem in continuatione disquisitionum arithmeticarum copiose tractabitur, hoc loco solas functiones circulares considerare visum est.*

Lecture 7

A proof by Gauss (beginning)

Recall that we want to show that z_1 is a root of the equation

$$Z^4 + Z^3 + Z^2 + Z + 1 = 0 \tag{I}$$

but of no equation of the forms

$$Z^3 + aZ^2 + bZ + c = 0 \tag{I}$$

$$Z^2 + aZ + b = 0 \tag{II}$$

$$Z + a = 0 \tag{III}$$

in which a, b c and d are fractions.

The impossibility of the last equation is clear because z_1 is not a fraction. If it were a root of the first, then using long division to divide (I) by $Z^3 + aZ^2 + bZ + c$, we would find

$$Z^4 + Z^3 + Z^2 + Z + 1 = (Z^3 + aZ^2 + bZ + c)(Z + d) + eZ^2 + fZ + g.$$

Substitute z_1 to find that z_1 is also a root of

$$eZ^2 + fZ + g = 0.$$

Then, as we just observed e is not 0, unless $e = f = g = 0$. If e is not 0, divide by it. Thus either

$$Z^4 + Z^3 + Z^2 + Z + 1 = (Z^3 + aZ^2 + bZ + c)(Z + d) \tag{IV}$$

or z_1 satisfies an equation of type (II). If it satisfies (II), then perform a long division to obtain

$$Z^4 + Z^3 + Z^2 + Z + 1 = (Z^2 + aZ + b)(Z^2 + cZ + d) + eZ + d.$$

Since $ez_1 + d$ cannot be 0 unless $e = d = 0$, we conclude that

$$Z^4 + Z^3 + Z^2 + Z + 1 = (Z^2 + aZ + b)(Z^2 + cZ + d). \tag{V}$$

Date of lecture: Fall term, December 9, 1999.

A proof by Gauss (continued)

We now show that the factorizations of (IV) and (V) are impossible. We first observe a very important fact.

An equation of degree n

$$Z^n + aZ^{n-1} + bZ^{n-2} + \cdots + d = 0 \tag{VI}$$

cannot have more than n roots!

Suppose (VI) has a root e. Using long division, divide by $Z - e$. The result is

$$Z^n + aZ^{n-1} + bZ^{n-2} + \cdots + d = (Z - e)(Z^{n-1} + AZ^{n-2} + \cdots + D) + f$$

Substitute e to see that $f = 0$. Now any other root e' not equal to e of (VI) must be a root of

$$Z^{n-1} + AZ^{n-2} + \cdots + D = 0, \tag{VII}$$

so that if (VI) had more than n roots, then (VII) would have more than $n - 1$. All we have to do now is continue, working our way down to lower and lower degree until we arrive at an equation of degree one

$$Z + \alpha = 0$$

that clearly has only one root.

General comments

The proof we present is a proof that can be extended without too much additional effort to the following statement.

Suppose p is a prime. Then the polynomial

$$Z^{p-1} + Z^{p-2} + Z^{p-3} + \cdots + Z + 1$$

admits no factorization.

This is a statement proved by Gauss in the *Disquisitiones*. We will need it for $p = 17$.

According to Bourbaki's *Éléments de l'histoire des mathématiques*, this was the first general statement of this sort about polynomials ever proved. It seems to me that in one sense, it is also the last. In the nature of things, there are very few large classes of polynomials that are all irreducible. On the other hand, if taken as a statement in the sense of Galois theory, as a statement affirming that the Galois group of the equation is large, then there are indeed other statements of this sort available and perhaps many more yet to be proved. The size and nature of Galois groups is a reasonably important mathematical topic, at least for mathematicians.

Since the proof in the general case is not so different from the proof for $p = 5$, we can expect a certain amount of sophistication.

A proof by Gauss (continued)

Suppose we had a factorization (IV). Since z_1, z_2, z_3 and z_4 are all roots of

$$Z^4 + Z^3 + Z^2 + Z + 1 = 0$$

each of them is either a root of

$$Z^3 + aZ^2 + bZ + c = 0 \tag{VIII}$$

or of

$$Z + d = 0$$

Since the latter is impossible, because $-d$ is, in contrast to z_1, z_2, z_3 and z_4, a fraction, they are all roots of (VIII) which gives (VIII) one root too many.

Thus we must have

$$Z^4 + Z^3 + Z^2 + Z + 1 = (Z^2 + aZ + b)(Z^2 + cZ + d) \tag{V}$$

The first thing is to establish that a, b, c and d are all integral. For this we need a little number theory. Suppose that one of these numbers is not integral. Then it is of the form

$$\frac{m}{n}, \qquad n \text{ positive, } n > 1$$

in which m and n have no common divisor. To be explicit, we write

$$\frac{3}{30}$$

as

$$\frac{1}{10} = \frac{1}{2 \times 5}$$

Thus there is some prime number p such that $n = rp^t$, $t > 0$, p does not divide r. For example, if $m/n = 1/10$ then p could be 5 and we would have $m = 1$, $r = 2$, $t = 1$.

We write each of a, b, c and d in this way.

$$a = \frac{a_1}{a_2 p^q}, \quad b = \frac{b_1}{b_2 p^r}, \quad c = \frac{c_1}{c_2 p^s}, \quad d = \frac{d_1}{d_2 p^t},$$

Suppose that at least one of the numbers q, r, s, t is positive. If, for example, $q = 0$ then p might divide a_1. Thus suppose that not all of a, b, c and d are integral. We multiply (IV) out to obtain

$$Z^4 + (a + c)Z^3 + (b + ac + d)Z^2 + (bc + ad)Z + bd = 0.$$

First of all, $a + c = 1$ is an integer. This is possible only if $q = s$, for if q is not equal to s then one of them is positive and larger than the other. The denominator of $a + c$ would contain the factor p^n if n is the larger of q and s. For example,

$$\frac{2}{3 \times 5^2} + \frac{3}{5} = \frac{2 + 9 \times 5}{3 \times 5^2} = \frac{47}{3 \times 5^2}.$$

We conclude that $q = s$.

Looking at $b + ac + d$, we next conclude that either $r = t$ or $q + s$ is equal to one of r or t. This line of argument quickly becomes confusing. The best thing is to follow Gauss and to prove a general theorem. Oddly enough, it is an argument that can best be explained in the general case. Here is what we want to show.

Suppose that the product of

$$Z^n + a_1 Z^{n-1} + a_2 Z^{n-2} + \cdots + a_{n-1} Z + a_n$$

and of

$$Z^m + b_1 Z^{m-1} + b_2 Z^{m-2} + \cdots + b_{m-1} Z + b_m$$

has integral coefficients and that all of the numbers a_i and b_j are fractions (and not some more complicated kind of irrational number!). Then all of the numbers a_i and b_j are integers.

We suppose not and choose a p that divides the denominator of at least one a_i or one b_j. Then we write

$$a_i = \frac{m_i}{n_i p^{r_i}} \qquad b_j = \frac{u_j}{t_j p^{s_j}}.$$

It is understood that p does not divide n_i and that it does not divide t_j. Starting with r_1, examine all the r_i and let r_k be the first that is at least as large as all the others. Thus r_k is bigger than those that came before and at least as large as those that come after. In the same way s_ℓ is to be larger than the s_j that come before and at least as large as those that come after.

The product is of degree $m+n$. we look at the coefficient of the power $Z^{m+n-k-\ell}$. It is

$$a_{m+n-k-\ell} b_0 + a_{m+n-k-\ell-1} b_1 + a_{m+n-k-\ell-2} b_2 + \cdots + a_0 b_{m+n-k-\ell}.$$

Some of these terms are purely fictive, those in which a_i appears with i larger than n or b_j with j larger than m. If a_0 or b_0 appear they are taken to be 1. For example, if $n = 5$, $m = 3$ then the coefficient of Z^4 is

$$a_4 + a_3 b_1 + a_2 b_2 + a_1 b_3.$$

In general, the coefficient of $Z^{k+\ell}$ is supposed integral and contains the term $a_k b_\ell$ in whose denominator $p^{r_k + s_\ell}$ occurs. It also contains terms like $a_{k-1} b_{\ell+1}$ whose denominator contains at most the factor $p^{r_\ell - 1 + s_\ell}$ or like $a_{k+1} b_{\ell-1}$ whose denominator contains at most the factor $p^{r_k + s_\ell - 1}$. Thus when we put everything over a common denominator, we will have a $p^{r_k + s_\ell}$ in the denominator that cannot be removed. This is a contradiction.

An example.

$$\left(Z^3 + \frac{1}{3} Z^2 + \frac{2}{9} Z + \frac{1}{9}\right) \times \left(Z^2 + \frac{4}{3} Z + \frac{7}{3}\right)$$

Here $k = 2$, $\ell = 1$, so that $m + n - k - \ell = 2$. The coefficient of Z^2 in the product is

$$\frac{1}{3}\frac{7}{3} + \frac{2}{9}\frac{4}{3} + \frac{1}{9} = \frac{7}{9} + \frac{8}{27} + \frac{1}{9} = \frac{21}{27} + \frac{8}{27} + \frac{3}{27} = \frac{32}{27}$$

Final step

We now know that in (V) the four numbers a, b, c and d are integral. The argument we used was taken from §42 of the *Disquisitiones*, thus from an early chapter. The next part is from §341, thus from a very late, indeed the last chapter, the one devoted to the division of the circle, thus to regular polygons. The number z_1 will be a root of

$$Z^2 + aZ + b = 0$$

or of

$$Z^2 + cZ + d = 0.$$

We can suppose that it is a root of the first. Then z_4, its complex conjugate will also be a root, so that the roots of the second are z_2 and z_3.

The polynomial $Z^2 + aZ + b$ is divisible by $Z - z_1$,

$$Z^2 + aZ + b = (Z - z_1)(Z - z_4) = Z^2 - (z_1 + z_4)Z + 1 = Z^2 - 2\cos(2\pi/5)Z + 1$$

which we write as

$$Z^2 - 2\cos(2\pi/5)Z + \cos^2(2\pi/5) + \sin^2(2\pi/5) = \big(Z - \cos(2\pi/5)\big)^2 + \sin^2(2\pi/5).$$

In the same way,

$$Z^2 + cZ + d = \big(Z - \cos(4\pi/5)\big)^2 + \sin^2(4\pi/5).$$

Thus if Z is an ordinary real number, both $Z^2 + aZ + b$ and $Z^2 + cZ + d$ are positive. If Z is an integer, they are integers.

Since

$$(Z^2 + aZ + b)(Z^2 + cZ + d) = Z^4 + Z^3 + Z^2 + Z + 1$$

we have first of all, for $Z = 1$,

$$(1 + a + b)(1 + c + d) = 5.$$

Thus one of these numbers is 1 and the other is 5. On the other hand,

$$Z^2 + aZ + b + Z^2 + cZ + d = 2Z^2 - (z_1 + z_2 + z_3 + z_4)Z + 2 = 2Z^2 + Z + 2$$

which is 5 when $Z = 1$. We conclude that $1 + 5 = 5$, which is out of the question.

545 INTELLIGENZBLATT 546
der
ALLGEM. LITERATUR-ZEITUNG
Numero 66.

Mittwochs den 1ten Junius 1796.

LITERARISCHE NACHRICHTEN.

I. Französische Literatur.

Zweyte Uebersicht.

Die für Paris bestimmten Mitglieder des grossen *Institut national* sind zwar in der letzten authentischen Nachricht aus Paris (S. *Intelligenzblatt* n. 19. S. 153 f.) schon so genau als möglich angegeben worden. Es dürfte aber in mehr als einer Rücksicht nicht uninteressant seyn, auch bey jeder Classe und Section die Namen derer bekannt zu machen, die blos *praesentirt* worden sind. Auch unter diesen sind viele im Auslande berühmte und geschätzte Namen, deren Verzeichniss hier wenigstens als Antinekrolog dienen, und zu mancherley Betrachtungen Anlass geben kann. So findet man z. B. unter diesen auch die Namen der Hr. v. *Villoison*, des Grafen *Gorani* und des einst mit Schrecken genannten *Hassenfratz*. Auch sind hier und da noch einige Berichtigungen hinzuzufügen:

I *Klasse.*

1. *Mathematik.* *Präsentirt* Lacroix.
2. *Mechanik.* Caroché, Molard, Bréguet, *Berthoud*, der zum wirklichen Mitgliede gewählt wurde, unterscheidet sich durch den Vornamen *Ferdinand*.
3. *Astronomie.* Le François.
4. *Experim. Phys.* Deparcieux, Carnot.
5. *Chimie.* Hassenfrax, Sequin, Baumé, Cadet.
6. *Natur-Hist. und Mineral.* Sage, Welter, Gillet l'Aumont, Faujas.
7. *Botanik.* La Billardière, Palissot de Beauvoi.
8. *Anatomie* und *Zoologie.* a) Pinel, Sue. b) Brugnières, Geoffroi, Olivier, Rose.
9. *Med. u. Chirurg.* a) Thouret, Cayes, la Tisse, Andry, Corvisar. b) Deschamps, Chaussier, Sue.
10. *Oeconomie* u. *Thierarzney.* a) André Michaut, Cretè Palluel, Dubois.

II *Klasse.*

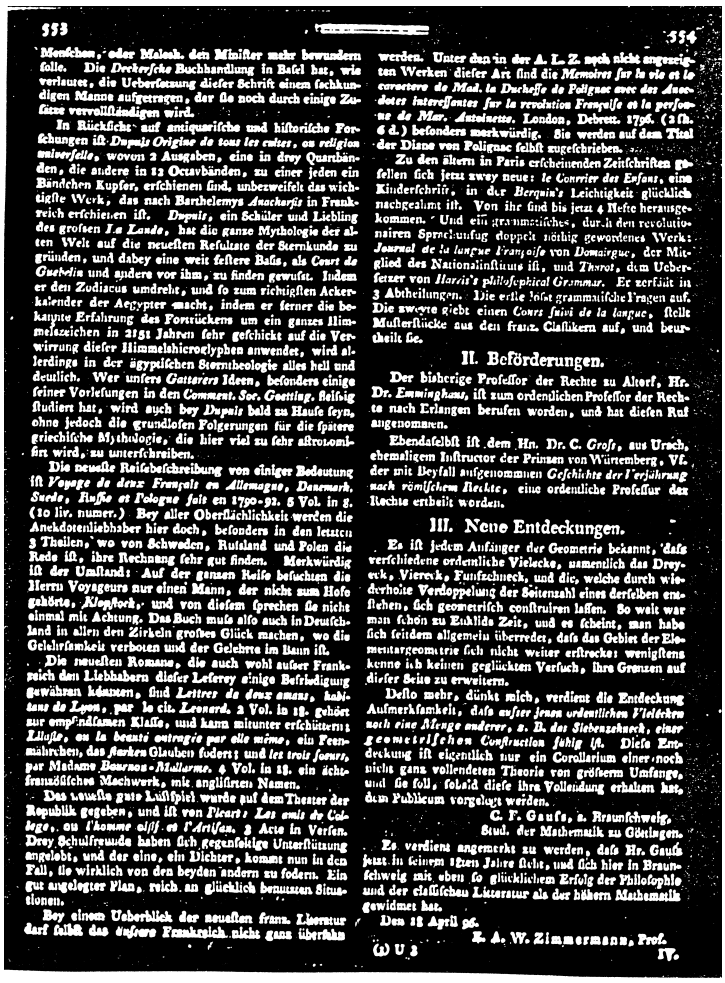
1. *Analyse der Empf.* Segond, La Romignière, La Salle.
2. *Moral.* La Bene, Villetarque, Blavet, Dinger, Rétif de la Bretonne, Ricard, Gorani.
4. *Gesetzgebung.* Treilhard.
5. *Polit. Oecon.* Jolivet, Otto: Farcos.
6. *Geschichte.* Garnier, Du Theil.
7. *Statistik* u. *Geographie.* Barbier du Bocage, Bèième, Bory, Rayneval, Bourgoin, Otto.

III *Klasse.*

1. *Grammatik.* Guerou, Lohier, Pougens, Binet, Marmontel, Palissot.
2. *Alte Sprachen.* Gail, Larcher, Voilloison, Maltor.
3. *Poesie.* Andrieux, Sedaine, Gailnava.
4. *Alterthümer.* Barthelemy, Millin.
5. *Mahlerey.* Gerard, Suvée, Giraudet.
6. *Bildhauerey.* Boizot, Gois.
7. *Baukunst.* Brognard, Molinos.
8. *Tonkunst,* Langlé, Le Sueur, Cherubini, Martini.
9. *Deklam.* Talma, La Rive.

Noch ist hierbey anzumerken, dass der berühmte Dichter *Delille*, aus dessen mit Sehnsucht erwarteten Gedicht *über die Einbildungskraft* so vortrefliche *Morceaux* im *Journal Encyclopedique* neuerlich gelesen worden sind, in einem mit ziemlicher Bitterkeit geschriebenen Brief sich für unfähig erklärt hat, die ihm zugedachte Mitgliedschaft anzunehmen. Er kann sich, wie es scheint, bey seiner erklärten Vorliebe für die alte Regierung noch nicht mit den neuen Formen aussöhnen. Der durch seine trefflichen Schauspiele, besonders durch den *vieux Célibataire* beliebte und beliebte *Collin d'Harleville* war in der Section der Grammatik statt *Garat*, der die Ernennung verbeten hatte, vom Directorium bestimmt worden. Als er von dieser Stelle Besitz nehmen wollte, kam die Section der Dichter, und bewies, dass er ihnen angehöre, und dass sie ihn schon zu ihrem Mitgliede erwählt hätten. Zweifach geehrt durch diese doppelte Ernennung folgte er dem Rufe seiner nähern Mitbruder, der Dichter, und trat in ihre Section ein. Und daran that er ganz recht, sagt ein Sprecher der öffentlichen Meinung, *un bon poëte fait plus qu'étudier et enseigner la langue: il la crée et l'enrichit.* Dieses wollten einst die Väter des Wörterbuchs der Academie nicht Wort haben.

Den 1sten Nivose (21. Decembr. 1795) hielten die 144 bis jetzt ernannten und bestätigten Mitglieder ihre *Seance d'ouverture*, die *Dusaulx* als Präsident nach dem Alter, durch Vorlesung des Gesetzes, wodurch das Institut seine Constitution erhält, eröffnete. *Delisle de la Salle* panegyrisirte hierauf die neue Einrichtung mit einer ziemlich ermüdenden Weitschweifigkeit. *Fourcroy* und *La Lande* thun Vorschläge wegen der Ernennung einzelner Ausschüsse, die von *Chenier* genauer bestimmt werden. *Laplace* dringt darauf, dass die Arbeiten der einzelnen



553

Menschen, oder Maleh. den Minister mehr bewundern solle. Die *Dreherische* Buchhandlung in Basel hat, wie verlautet, die Uebersetzung dieser Schrift einem sachkundigen Manne aufgetragen, der sie noch durch einige Zusätze vervollständigen wird.

In Rücksicht auf antiquarische und historische Forschungen ist *Dupuis Origine de tous les cultes, ou religion universelle*, wovon 2 Ausgaben, eine in drey Quartbänden, die andere in 12 Octavbänden, zu einer jeden ein Bändchen Kupfer, erschienen sind, unbezweifelt das wichtigste Werk, das nach Barthelemys *Anacharsis* in Frankreich erschienen ist. *Dupuis*, ein Schüler und Liebling des grossen *La Lande*, hat die ganze Mythologie der alten Welt auf die neuesten Resultate der Sternkunde zu gründen, und dabey eine weit festere Basis, als *Court de Gebelin* und andere vor ihm, zu finden gewusst. Indem er den Zodiacus umdreht, und so zum richtigsten Ackerkalender der Aegypter macht, indem er ferner die bekannte Erfahrung des Forstrückens um ein ganzes Himmelszeichen in 2151 Jahren sehr geschickt auf die Verwirrung dieser Himmelshieroglyphen anwendet, wird allerdings in der ägyptischen Sternbeologie alles hell und deutlich. Wer unsers *Gatterers* Ideen, besonders einige seiner Vorlesungen in den *Comment. Soc. Goetting.* fleissig studiert hat, wird auch bey *Dupuis* bald zu Hause seyn, ohne jedoch die grundlosen Folgerungen für die spätere griechische Mythologie, die hier viel zu sehr astronomisirt wird, zu unterschreiben.

Die neueste Reisebeschreibung von einiger Bedeutung ist *Voyage de deux Français en Allemagne, Danemark, Suede, Russie et Pologne fait en 1790-92.* 8 Vol. in 8. (10 liv. numer.) Bey aller Oberflächlichkeit werden die Anekdotenliebhaber hier doch, besonders in den letzten 3 Theilen, wo von Schweden, Rußland und Polen die Rede ist, ihre Rechnung sehr gut finden. Merkwürdig ist der Umstand: Auf der ganzen Reise besuchten die Herrn Voyageurs nur einen Mann, der nicht zum Hofe gehörte, *Klopstock*, und von diesem sprechen sie nicht einmal mit Achtung. Das Buch muß also auch in Deutschland in allen den Zirkeln grosses Glück machen, wo die Gelehrsamkeit verboten und der Gelehrte im Bann ist.

Die neuesten Romane, die auch wohl ausser Frankreich den Liebhabern dieser Lesery einige Befriedigung gewähren können, sind *Lettres de deux amans, habitans de Lyon*, par le cit. *Leonard*. 2 Vol. in 12. gehört zur empfindsamen Klasse, und kann mitunter erschüttern; *Lilotte, ou la beauté outragée par elle même*, ein Feenmährchen, das *starken* Glauben fodert; und *les trois sœurs*, par Madame *Bourson-Malherne*. 4 Vol. in 12. ein ächtfranzösisches Machwerk, mit anglisirten Namen.

Das neueste gute Lustspiel wurde auf dem Theater der Republik gegeben, und ist von *Fleurt*: *Les amis de Collège, ou l'homme aisé et l'artiste*. 3 Acte in Versen. Drey Schulfreunde haben sich gegenseitige Unterstützung angelobt, und der eine, ein Dichter, kommt nun in den Fall, sie wirklich von den beyden andern zu fodern. Ein gut angelegter Plan, reich an glücklich benutzten Situationen.

Bey einem Ueberblick der neuesten franz. Literatur darf selbst das *ärmere* Frankreich nicht ganz übersehen

554

werden. Unter den in der A. L. Z. noch nicht angezeigten Werken dieser Art sind die *Memoires sur la vie et la correspondance de Mad. la Duchesse de Polignac avec des Anecdotes intéressantes sur la revolution Française et la personne de Mar. Antoinette.* London, Debrett. 1796. (2 fl. 6 d.) besonders merkwürdig. Sie werden auf dem Titel der Dame von Polignac selbst zugeschrieben.

Zu den ältern in Paris erscheinenden Zeitschriften gesellen sich jetzt zwey neue: *le Courrier des Enfans*, eine Kinderschrift, in der *Berquin's* Leichtigkeit glücklich nachgeahmt ist. Von ihr sind bis jetzt 4 Hefte herausgekommen. Und ein grammatisches, durch den revolutionairen Sprachunfug doppelt nöthig gewordenes Werk: *Journal de la langue Française* von *Domairgue*, der Mitglied des Nationalinstituts ist, und *Thurot*, dem Uebersetzer von *Harris's philosophical Grammar*. Er zerfällt in 3 Abtheilungen. Die erste löst grammatische Fragen auf. Die zweyte giebt einen *Cours fixé de la langue*, stellt Musterstücke aus den franz. Classikern auf, und beurtheilt sie.

II. Beförderungen.

Der bisherige Professor der Rechte zu Altorf, Hr. Dr. *Ennninghaus*, ist zum ordentlichen Professor der Rechte nach Erlangen berufen worden, und hat diesen Ruf angenommen.

Ebendaselbst ist dem Hn. Dr. C. *Groß*, aus Urach, ehemaligem Instructor der Prinzen von Würtemberg, Vf. der mit Beyfall aufgenommen *Geschichte der Verjährung nach römischem Rechte*, eine ordentliche Professur des Rechts ertheilt worden.

III. Neue Entdeckungen.

Es ist jedem Anfänger der Geometrie bekannt, daß verschiedene ordentliche Vielecke, namentlich das Dreyeck, Viereck, Funfzehneck, und die, welche durch wiederholte Verdoppelung der Seitenzahl eines derselben entstehen, sich geometrisch construiren lassen. So weit war man schon zu Euklids Zeit, und es scheint, man habe sich seitdem allgemein überredet, daß das Gebiet der Elementargeometrie sich nicht weiter erstrecke: wenigstens kenne ich keinen geglückten Versuch, ihre Grenzen auf dieser Seite zu erweitern.

Desto mehr, dünkt mich, verdient die Entdeckung Aufmerksamkeit, daß *außer jenen ordentlichen Vielecken noch eine Menge anderer*, z. B. das *Siebenzehneck, einer geometrischen Construction fähig ist*. Diese Entdeckung ist eigentlich nur ein Corollarium einer noch nicht ganz vollendeten Theorie von grösserm Umfange, und sie soll, sobald diese ihre Vollendung erhalten hat, dem Publicum vorgelegt werden.

C. F. Gauß, a. Braunschweig,
Stud. der Mathematik zu Göttingen.

Es verdient angemerkt zu werden, daß Hr. Gauß jetzt in seinem 19ten Jahre steht, und sich hier in Braunschweig mit eben so glücklichem Erfolg der Philosophie und der classischen Litteratur als der höhern Mathematik gewidmet hat.

Den 18 April 96.

K. A. W. Zimmermann, Prof.

III. Neue Entdeckungen

Es ist jedem Anfänger der Geometrie bekannt, dass verschiedene ordentliche Vielecke, namentlich das Dreyeck, Viereck, Funfzehneck, und die, welche durch wiederholte Verdoppelung der Seitenzahl eines derselben entstehen, sich geometrisch construiren lassen. So weit war man schon zu Euklids Zeit, und es scheint, man habe sich seitdem allgemein überredet, dass das Gebiet der Elementargeometrie sich nicht weiter erstrecke: wenigstens kenne ich keinen geglückten Versuch, ihre Grenzen auf dieser Seite zu erweiten.

Desto mehr, dünkt mich, verdient die Entdeckung Aufmerksamkeit, dass *ausser jenen ordentlichen Vielecken noch eine Menge anderer, z.B., das Siebenzehneck, einer geometrischen Konstruction fähig ist*. Diese Entdeckung ist eigentlich nur ein Corollarium einer noch nicht ganz vollendeten Theorie von grösserem Umfange, und sie soll, sobald diese ihre Vollendung erhalten hat, dem Publicum vorgelegt werden.

C. F. Gauss, a. Braunschweig,
Stud. der Mathematik zu Göttingen.

Es verdient angemerkt zu werden, dass Hr. Gauss jetzt in seinem 18ten Jahr steht, und sich hier in Braunschweig mit eben so glücklichem Erfolg der Philosophie und der classischen Litteratur als der höheren Mathematik gewidmet hat.

Den 18 April 96.

E. A. W. Zimmermann, Prof.

Die Allgemeine Literatur-Zeitung

From Meyers Enzyklopädisches Lexikon:

This review appeared in Jena from 1785 to 1803 and in Halle from 1804 to 1849 and was a leading organ of German classical and romantic literature. Goethe, Schiller and Kant were among the editors and authors. It moved to Halle as a result of an effort of the romantics to increase their control over the review and was replaced in Jena, on the initiative of Goethe by the Jenaische Allgemeine Literatur-Zeitung.

Gauss

Gauss, who was born in 1777, wrote the *Disquisitiones* between 1796 and 1798, thus between his nineteenth and twenty-first years. It did not appear until 1801. It contains a great deal in the way both of theorems and theories, the most important being:

1. Proof of law of quadratic reciprocity. The statement was already known at the time, but even the best of the eighteenth century mathematicians were unable to find a proof. It remains a central mathematical theorem.

2. Developed the theory of binary quadratic forms. In particular, he introduced the notion of composition of quadratic forms and established its properties. Although in some respects, namely in the context of the notion of ideal number, composition has become a common working tool of all algebraists and number-theorists, Gauss's theory itself is still difficult and little known. His form of the theory would appear to be that best suited to computation.

3. Cyclotomic fields. The construction of the regular heptadecagon, and, more generally, the analysis of the numbers formed from roots of unity. This is thus one of the earliest manifestations of Galois theory. Gauss presumably knew more than he included in the book, but he, apparently, published very little more on the subject.

His thesis of 1799 established, in effect and for the first time, that every polynomial equation has a root.

$$Z^n + aZ^{n-1} + bZ^{n-2} + \cdots + d = 0.$$

As the root may be complex and the thesis did not refer to complex numbers, the formulation of the thesis was necessarily somewhat different. I have already emphasized that this is a basic mathematical fact.

These are all theories and results to which the contributions of Gauss are clear. In addition, he appears to have occupied himself as a very young man, even as an adolescent, with other important problems and observations, for example, with the nature of geometries in which the parallel axiom of Euclid is not satisfied and with the arithmetic-geometric mean, which is both an elementary and an advanced topic. Here, however, the evidence is different. It consists of Gauss's recollections as a somewhat saturnine older man, so that it appears to be difficult to disentangle what he himself discovered later, what he learned from other authors as an adolescent—he had an early and extensive acquaintance with the work of various leading eighteenth century mathematicians—as well as what he learned later, from what he discovered early. One could certainly spend a lot of time with Gauss's Collected Works and with his correspondence, reflecting on these matters.

One extremely useful reference is a diary that Gauss kept between 1796 and 1814, with 146 entries that record his principal discoveries. The lemniscate function to which, as I noticed, Gauss alludes in the first lines of chapter 7 of the *Disquisitiones* appears several times. I was asked what Gauss may have meant with his allusion to the lemniscate. A brief examination of the diary and of the collected works, which contain ample editorial comments, makes perfectly clear what Gauss knew. Although it is a digression from my main purpose, it is worthwhile to tarry a little on the matter.

The goal of this year's lectures is after all to communicate, starting at the beginning, some genuine mathematical understanding, beyond the gee-whiz or what I refer to as the Jack Horner manner, of recent achievements in number theory, and it would be a shame, since we are now in a position to appreciate a more detailed explanation of Gauss's allusion, to let slip the occasion of acquiring more concrete information.

Gauss was an overwhelming presence in nineteenth century mathematics, Even though he exerted little active influence. The German pre-eminence in mathematics as a whole, and in certain domains such as number theory in particular, that lasted throughout the nineteenth century and until the early thirties is due in good part to him, although the Prussian university system was probably also a significant factor. I have not studied these matters. Oddly enough it appears to have been André Weil who was most thoroughly imbued with the aspirations of German number theory, both through direct, personal experience as a young man during the twenties and through his studies of various nineteenth century authors. Simplifying, for the purposes of brevity, an elaborate development in which a large number of mathematicians took part, one might say that he not only brought it intact through the war at its highest level but also was the principal source of its transformation into the theories that were finally and successfully exploited in the proof of Fermat's theorem.

His major contribution was, oddly enough, a set of conjectures, the Weil conjectures, now demonstrated, but by others. He is, in various comments to his papers, quite explicit about the relation of these conjectures to Gauss and the lemniscate.

I quote from Weil's *Two lectures on number theory, past and present*, an essay I recommend to your attention.

> *In 1947, in Chicago, I felt bored and depressed and, not knowing what to do, I started reading Gauss's two memoirs on biquadratic residues, which I had never read before. . . . This led me in turn to some conjectures.*

A few lines later Weil draws attention to the very last entry in Gauss's diary, an entry to which we shall come in a moment.

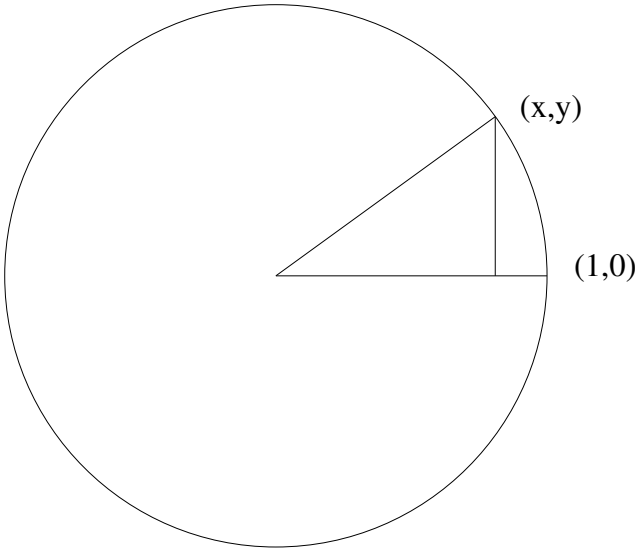
$$Z^n + aZ^{n-1} + bZ^{n-2} + \cdots + d = 0$$

Digression

The digression at first sight seems to demand some knowledge of the calculus, but it does not. I first write down a formula that may be familiar to some, but not to all. No matter! Do not puzzle over the left side. It is no more than the mathematician's usual fastidious way of writing down the length of the arc from the point $(1,0)$ on the circle to the point (x,y) and that is what we mean by θ, which of course has to be measured in radians, thus in units in which the radius is 1, but that is the unit chosen. If

$$\int_0^y \frac{dt}{\sqrt{1-t^2}} = \theta, \tag{A}$$

then $y = \sin(\theta)$. If $y = 1$ then $\theta = \pi/2$.



We now do something similar for the lemniscate, a curve defined by the equation

$$(x^2+y^2)^2 - (x^2-y^2) = 0$$

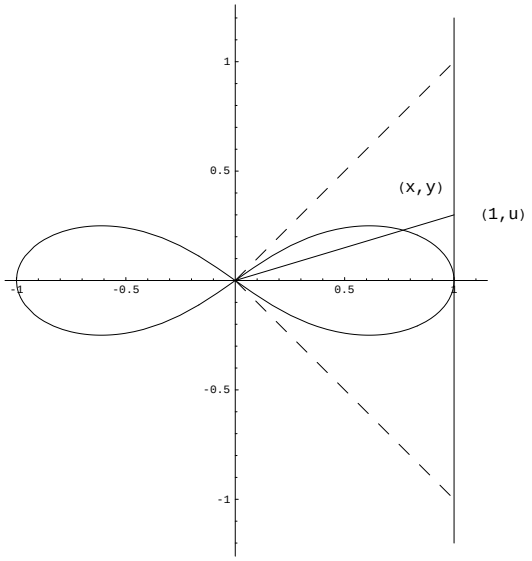
The lemniscate is the curve in the form of a bow. The point (x,y) is the point where the line through the points $(0,0)$ and $(1,u)$ cut the curve. The length of the curve from $(1,0)$ to the point (x,y) is expressed mathematically as

$$\int_0^u \frac{dt}{\sqrt{1-t^4}} = \theta. \tag{B}$$

Once again, there is no need to be troubled by the integral. It is again just a way of expressing the length of an arc of a curve. Observe that θ plays here the role of the angle in a circle measured in radians. Gauss wrote

$$u = \sin\operatorname{lemn}(\theta).$$

If $u = 1$, then θ is some number that I call, following Gauss, $\varpi/2$. Thus $\varpi/2$ is the length of the upper loop on the right running from $(1,0)$ to $(0,0)$.



$$x = \frac{\sqrt{1-u^2}}{1+u^2} \quad y = \frac{u\sqrt{1-u^2}}{1+u^2}$$

Constructing a regular triangle, a regular pentagon, or a regular heptadecagon is the problem of dividing the total circumference of the circle into three, five or seventeen arcs of equal length. We could consider the same problem for the lemniscate, taking the initial point, which is now important as it was not, because of symmetry, for the circle, to be the point $(0, 1)$. In an entry for March 19, 1797 Gauss notes that this leads to an equation for u of degree m^2, whereas for the circle it was an equation of degree m. In the cases already considered, m was 3 or 5. We remove one easy root, $u = 0$ corresponding to the first point of division. This leads to equations of degree $m - 1$ or for a lemniscate $m^2 - 1$. In a later entry, apparently for April 15, he observes there is a problem of separating the real roots of this equation from the complex. He is seeking the real roots. The corresponding equation for the circle, thus for y, has only real roots. It is the numbers $x + iy$ that are complex. The real roots of the equation of degree $m^2 - 1$ give the division points and there are $m - 1$ of them.

In an entry dated March 21, he observes implicitly (all the entries are cryptic) that these $m-1$ roots are numbers that can be constructed with a ruler and compass.

Lemniscata geometrice in quinque partes dividitur

The young Norwegian mathematician Abel published in 1827 and 1828 proofs of the assertions implicit in Gauss's remark in the *Disquisitiones*. For $m = 3$, 5 the necessary constructions had been found much earlier, by 1750, by the Italian geometer Count Fagnano.

The connections of the lemniscate with number theory are too ramified for us to discuss them in any more detail. The division points were important then and are important now, but so are what are called congruences modulo a prime. The

two topics are very closely related. I end with the entry to which Weil alluded, the very last in the diary, dated July 9, 1814.

[III.]

[TEILUNG DER LEMNISKATE.]

[Eintragungen im LEISTE.]

[1.]

[S. 69]

Die Theilung der Lemniscata in sieben Theile gibt die Gleichung:

$$16(1-x^4)\left(\begin{matrix}1 & -5 & -5 & +1 \\ 1 & +20 & -26 & +20 & +1\end{matrix}\right)^2 = \left(\begin{matrix}3 & *-6 & *-1 \\ 1 & *+6 & *-3\end{matrix}\right)^4.$$

[2.]

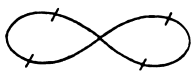
[S. 87]

Sit $\sin\frac{1}{7}kR = \langle k\rangle$, tum habebuntur aequationis radices (0), $\pm\langle 4\rangle$, $\pm\langle 2\rangle$,

$$\frac{(0)+(5)(4)(1)\sqrt{-1}}{(1)-(0)(5)\ldots}$$

$$\frac{\langle 4\rangle+(1)(4)(1)\sqrt{-1}}{(1)-(4)(4)(1)\sqrt{-1}}$$

$$\frac{(2)-(3)(4)(1)\sqrt{-1}}{(1)+(2)(3)(4)\sqrt{-1}}$$



$$\pm 1,\ \sqrt{-1}\left[\begin{matrix}(0) \\ (2) \\ (4)\end{matrix}\right| \left.\begin{matrix}\frac{(4)}{(1)}\cdot\frac{1+(1)(1)\sqrt{-1}}{1-(4)(4)\sqrt{-1}} \\ \frac{(2)}{(3)}\ \frac{1+(3)(3)\sqrt{-1}}{1-(2)(2)\sqrt{-1}}\end{matrix}\right|$$

[3.]

[S. 90—91]

		[cos 18°]
		0,965425785 [= μ 18°]
		1,034180311 [= ν 18°]
1	1,31102877 $\left[=\frac{\varpi}{2}\right]$	sin 36°
2	1,71879545	0,524411511 $\left[=\frac{\varpi}{5}\right]$
4	2,95416	— 661011
5	3,87311	— 292
6	5,07777	0,523750208 [= M 36°]
8	8,72765	1,006302208 $\left[=1+\frac{1}{12}\left(\frac{\varpi}{5}\right)^4\right]$
9	11,44320	— 567
10	15,00	[1,006301641 = N 36°]

[sin] 36° =

$\frac{0,523750208}{1,006301641} = 0,5204703904.$

[sin] 72° = cos 18°

$\frac{0,965425785}{1,034180311} = 0,9335177577.$

[4.]

[S. 102]

Die Theilung der Lemniscata in 5 Theile führt auf diese Gleichung

$$\frac{9-36x^4+30x^8+12x^{12}+x^{16}}{1+12x^4+30x^8-36x^{12}+9x^{16}} = \frac{4(1-x^4)}{1+2x^4+x^8}$$

$$\left.\begin{array}{rrrrrrr}
9 & -36 & +30 & +12 & +1 & & \\
 & +18 & -72 & +60 & +24 & +2 & \\
 & & +9 & -36 & +30 & +12 & +1 \\
-4 & -48 & -120 & +144 & -36 & & \\
 & +4 & +48 & +120 & -144 & +36 & \\
\hline
5 & -62 & -105 & +300 & -125 & +50 & +1
\end{array}\right\} = 0.$$

[Wurzeln dieser Gleichung vom 24. Grade sind $\sin \operatorname{lemn} \frac{k\varpi}{5}$ für $k = 1, 2, 3, 4$, die übrigen sind imaginär, also:]

Determ. rad. imag.

$$\frac{\square}{\square} = \frac{4.1 - x^4)}{\square},$$

[setze $x^4 = y$, so ist]

$$(3 - 6y - yy)(1 + y) = 2(1 + 6y - 3yy)\sqrt{(1 - y)}$$

$$S = \sqrt{720} - 26 \; [= 12\sqrt{5} - 26]$$

$$\left[= \left(\sin \operatorname{lemn} \tfrac{2\varpi}{5}\right)^4 + \left(\sin \operatorname{lemn} \tfrac{4\varpi}{5}\right)^4\right]$$

$$\begin{array}{l} 349 - 156\sqrt{5} \\ -9 + \quad 4\sqrt{5} \\ \hline 340 - 152\sqrt{5} \end{array} \left[= \tfrac{1}{2}\left(\sin \operatorname{lemn} \tfrac{4\varpi}{5}\right)^4 - \tfrac{1}{2}\left(\sin \operatorname{lemn} \tfrac{2\varpi}{5}\right)^4\right]^2.$$

Zwei Wurzeln obiger Gleichung sind

$$+ 0{,}0733810047 \; \left[= \left(\sin \operatorname{lemn} \tfrac{2\varpi}{5}\right)^4\right]$$

$$+ 0{,}7594355 \quad \left[= \left(\sin \operatorname{lemn} \tfrac{4\varpi}{5}\right)^4\right].$$

[5.]

[S. 100–101]

Auflösung der Gleichung

$$5 - 62x - 105xx + 300x^3 - 125x^4 + 50x^5 + x^6 \; [= 0^*)]$$

[Es folgt eine Zahlenrechnung, anscheinend nach der Regula falsi].

Also eine Wurzel

$$= 0{,}07338100477 \; \left[= \left(\sin \operatorname{lemn} \tfrac{2\varpi}{5}\right)^4\right]$$

und folglich

$$\sin 36^0 = 0{,}52047024 \; [= \sqrt[4]{0{,}073381}].$$

[*) Das x in dieser Gleichung ist die vierte Potenz der im art. [4.] ebenso bezeichneten Unbekannten; die Gleichung hat also die Wurzeln $\left(\sin \operatorname{lemn} \frac{k\varpi}{5}\right)^4$ für $k = 1, 2, 3, 4$.]

Hieraus aber folgt eine zweite Wurzel

$$= 16\,\frac{(1-t^2)t}{(1+t^2}$$

$l16 = 1{,}2041200$

$lt = 0{,}8655836 - 2$ [$= \log_{10} 0{,}073381\ldots = \log_{10}(\sin \text{lemn } 36^0)^4$]

$l(1-t)^2 = 0{,}9338025 - 1$

$-l(1+t)^2 = 0{,}8769844 - 1$

$0{,}8804905 - 1$ [$= \log_{10}$] $0{,}7594348$ [$= \log_{10}(\sin \text{lemn } 72^0)^4$].

Also

$$l \sin 72^0 = 0{,}9701226$$

und

$$\sin 72^0 = 0{,}9335179.$$

[6.]

[Ein Zettel Fh Nr. 1, Kapsel 50.]

Rechnungen zur Lemniscata gehörig.

$(\sin 0{,}4)^4 + (\sin 0{,}8)^4 = 12\sqrt{5} - 26$ [*)]

$= 2(0{,}4164078649\quad 9873817845\quad 5042012387\quad 65741)$

$(\frac{1}{2}(\sin 0{,}8)^4 - \frac{1}{2}(\sin 0{,}4)^4)^2 = 340 - 152\sqrt{5}$

$= 0{,}1176674200\quad 3196614580\quad 5602352846\quad 01228.$

Daraus Radix

$0{,}3430268503\quad 0761971797\quad 7310507555\quad 85731$

$-0463415326\quad 98758$

$6847092228\quad 86973$

Also

$(\sin 0{,}4)^4 = 0{,}0733810146\quad 9111846047\quad 7731504831\quad 80010$

Daraus Radix

$(\sin 0{,}4)^2 = 0{,}2708893033\quad 8999814497\quad 30710$

[*) $\sin 0{,}4$ und $\sin 0{,}8$ bedeuten $\sin \frac{4\varpi}{10}$ und $\sin \frac{8\varpi}{10}$, d. h. also $\sin \text{lemn} \frac{2\varpi}{5}$ und $\sin \text{lemn} \frac{4\varpi}{5}$.]

Observatio per inductionem facta gravissima theoriam residuorum biquadraticorum cum functionibus lemniscatis elegantissime nectens. Puta si $a+bi$ est numerus primus, $a-1+bi$ per $2+2i$ divisibilis, multitudo omnium solutionum congruentiae

$$1 \equiv xx + yy + xxyy \pmod{a+bi}$$

inclusis

$$x = \infty, \quad y = \pm i; \qquad x = \pm i, \quad y = \infty,$$

fit

$$= (a-1)^2 + bb.$$

We have progressed a little beyond this last entry in the intervening 185 years, but not so much as one might think! Without going into further detail, which would be too much of a digression, I observe that if

$$1 = x^2 + y^2 + x^2y^2$$

and

$$z = y(1+x^2)$$

then

$$z^2 = y^2(1+2x^2+x^4) = y^2(1+x^2) + y^2x^2(1+x^2) = 1 - x^2 + x^2(1-x^2) = 1 - x^4.$$

Comments

I return to the observation that was the occasion for this digression, as it could be misunderstood. I prefer that it not be, for the point I was attempting to make is serious.

We have seen, when discussing the regular pentagon the importance, or at least the interest, of the algebraic symmetries of points that divide the circle into five equal arcs. We expect something similar for the regular heptadecagon. We have also observed, without entering into the mathematical details, that a similar interest, for similar reasons, attaches to the points that divide a lemniscate into five equal parts, although the equations here are more difficult to come by. The modern mathematical catch phrase for the symmetries is "Galois structure" or "Galois action" and the phrase, or theory, that captures the division into equal parts is "ℓ-adic cohomology". Thus we have studied—just a little—the "Galois action on ℓ-adic cohomology". This is part, a good part, of the context in which Wiles's proof of the Fermat theorem is carried out. So we have succeeded—again just a little—in coming into direct contact with the mathematics itself, rather than with a publicist's rendering of it. Just as the public at large is separated from the essential ideas by the popularizers, who hear and repeat the catch phrases, often without understanding their content, mathematicians, even those with some special competence, are often separated from it by the accretion of theory. Rather than returning to the specific and tangible to communicate, we resort to metaphors, which only take the abstraction one degree further.

The last entry in the diary refers, although in a manner that is cryptic enough that we cannot be entirely sure what Gauss had in mind (but Abel's paper permits a precise guess), to a second aspect of modern number theory, to congruences, thus to the study of the number of solutions of a relation

$$p \text{ divides } P(x, y, z, \dots).$$

We may not have occasion to say much about the second topic. As Gauss suggests, the two are linked. The connection has become such a commonplace in contemporary mathematics that we forget how strange it is. It would be good, if we have the time, to return to it, to try to capture some of its wonder.

Lecture 8

The heptadecagon: beginning

We have seventeen seventeenth roots of 1. We take them to be

$$z_k = \cos(2k\pi/17) + i\sin(2k\pi/17), \qquad k = 0, \ldots, 16.$$

As before $z_0 = 1$ and each of the others satisfies the equation

$$Z^{16} + Z^{15} + Z^{14} + Z^{13} + Z^{12} + \cdots + Z^6 + Z^5 + Z^4 + Z^3 + Z^2 + Z^1 + 1 = 0.$$

We take as proved that they satisfy no equation of smaller degree. This is proved pretty much as it was for the fifth roots of unity. Thus all the numbers

$$a_1 z_1 + a_2 z_2 + a_3 z_3 + a_4 z_4 + \cdots + a_{13} z_{13} + a_{14} z_{14} + a_{16} z_{16}$$

are different. We must not forget that

$$z_1 + z_2 + z_3 + z_4 + \cdots + z_{13} + z_{14} + z_{15} + z_{16} = -1.$$

Moreover we have sixteen symmetries $z_1 \to z_2$, $z_1 \to z_3$, $z_1 \to z_4$, and so on. If the symmetry takes z_1 to z_2 then it takes $z_5 = z_1^5$, for example, to $z_2^5 = (z_1^2)^5 = z_1^{10}$. It takes z_9 to $z_2^9 = z_1^{18} = z_1^1$. We call this symmetry, thought of as a reflection, ρ and ask what happens when we repeat it over and over again, as in a hall of mirrors. It is enough to trace its effect on z_1 because all the other numbers can be expressed by taking powers of z_1, multiplying them by fractions, and adding the results together. This can be done after the reflection as well as before. The result is not changed. In each line of the table on the next page, the first step is the result of the preceding line and the second is the result of then applying ρ one more time.

$$\begin{aligned}
\rho &: && z_1 \to z_2 \\
\rho^2 &: && z_1 \to z_2, && z_2 \to z_4 \implies z_1 \to z_4 \\
\rho^3 &: && z_1 \to z_4, && z_4 \to z_8 \implies z_1 \to z_8 \\
\rho^4 &: && z_1 \to z_8, && z_8 \to z_{16} \implies z_1 \to z_{16} \\
\rho^5 &: && z_1 \to z_{16}, && z_{16} \to z_{15} \implies z_1 \to z_{15} \\
\rho^6 &: && z_1 \to z_{15}, && z_{15} \to z_{13} \implies z_1 \to z_{13} \\
\rho^7 &: && z_1 \to z_{13}, && z_{13} \to z_9 \implies z_1 \to z_9 \\
\rho^8 &: && z_1 \to z_9, && z_9 \to z_1 \implies z_1 \to z_1
\end{aligned}$$

Thus after eight repetitions we come to the trivial symmetry. The number z_1 is reflected in itself, as are therefore all other numbers.

So we start again, this time with σ which reflects z_1 in z_3. Thus it takes $z_3 = z_1^3$ to $z_3^3 = z_1^9$.

Date of lecture: Fall term, December 14, 1999.

$$
\begin{aligned}
\sigma: &\quad z_1 \to z_3 \\
\sigma^2: &\quad z_1 \to z_3, && z_3 \to z_9 \implies z_1 \to z_9 \\
\sigma^3: &\quad z_1 \to z_9, && z_9 \to z_{10} \implies z_1 \to z_{10} \\
\sigma^4: &\quad z_1 \to z_{10}, && z_{10} \to z_{13} \implies z_1 \to z_{13} \\
\sigma^5: &\quad z_1 \to z_{13}, && z_{13} \to z_5 \implies z_1 \to z_5 \\
\sigma^6: &\quad z_1 \to z_5, && z_5 \to z_{15} \implies z_1 \to z_{15} \\
\sigma^7: &\quad z_1 \to z_{15}, && z_{15} \to z_{11} \implies z_1 \to z_{11} \\
\sigma^8: &\quad z_1 \to z_{11}, && z_{11} \to z_{16} \implies z_1 \to z_{16} \\
\sigma^9: &\quad z_1 \to z_{16}, && z_{16} \to z_{14} \implies z_1 \to z_{14} \\
\sigma^{10}: &\quad z_1 \to z_{14}, && z_{14} \to z_8 \implies z_1 \to z_8 \\
\sigma^{11}: &\quad z_1 \to z_8, && z_8 \to z_7 \implies z_1 \to z_7 \\
\sigma^{12}: &\quad z_1 \to z_7, && z_7 \to z_4 \implies z_1 \to z_4 \\
\sigma^{13}: &\quad z_1 \to z_4, && z_4 \to z_{12} \implies z_1 \to z_{12} \\
\sigma^{14}: &\quad z_1 \to z_{12}, && z_{12} \to z_2 \implies z_1 \to z_2 \\
\sigma^{15}: &\quad z_1 \to z_2, && z_2 \to z_6 \implies z_1 \to z_6 \\
\sigma^{16}: &\quad z_1 \to z_6, && z_6 \to z_1 \implies z_1 \to z_1
\end{aligned}
$$

Thus the powers of σ exhaust the symmetries and we can measure the amount of symmetry of any element

$$\text{(A)} \qquad a_1z_1 + a_2z_2 + a_3z_3 + a_4z_4 + \cdots + +a_{13}z_{13} + a_{14}z_{14} + a_{15}z_{15} + a_{16}z_{16}$$

by the smallest power of σ under which it is invariant. For example the most symmetric are those that are their own reflections by σ and therefore by any repetition of σ. The reflection of (A) given by σ is

$$a_1z_3 + a_2z_6 + a_3z_9 + a_4z_{12} + \cdots + a_{13}z_5 + a_{14}z_8 + a_{15}z_{11} + a_{16}z_{14}.$$

What happens is that it can be invariant only if all coefficients are the same. But

$$az_1 + az_2 + az_3 + \cdots = -a$$

so that if it is invariant under σ itself, it is just a fraction or rational number. If it is invariant under σ^2, it must be a sum $a(8,1) + b(8,3)$ where, following Gauss and using his notation, we build the periods

$$(8,1) = z_1 + z_9 + z_{13} + z_{15} + z_{16} + z_8 + z_4 + z_2$$

and

$$(8,3) = z_3 + z_{10} + z_5 + z_{11} + z_{14} + z_7 + z_{12} + z_6.$$

Since

$$(8,1) + (8,3) = -1$$

and $(8,1)^2$ has the same symmetry as $(8,1)$, we must have

$$(8,1)^2 = a(8,1) + b(8,3) = (a-b)(8,1) + b.$$

Once we have calculated a and b we will be able to solve easily for $(8,1)$.

The calculation is somewhat lengthy because $(8,1)\times(8,1)$ contains sixty-four terms. Let's see what can be done.

	z_1	z_9	z_{13}	z_{15}	z_{16}	z_8	z_4	z_2
z_1	z_2	z_{10}	z_{14}	z_{16}	1	z_9	z_5	z_3
z_9	z_{10}	z_1	z_5	z_7	z_8	1	z_{13}	z_{11}
z_{13}	z_{14}	z_5	z_9	z_{11}	z_{12}	z_4	1	z_{15}
z_{15}	z_{16}	z_7	z_{11}	z_{13}	z_{14}	z_6	z_2	1
z_{16}	1	z_8	z_{12}	z_{14}	z_{15}	z_7	z_3	z_1
z_8	z_9	1	z_4	z_6	z_7	z_{16}	z_{12}	z_{10}
z_4	z_5	z_{13}	1	z_2	z_3	z_{12}	z_8	z_6
z_2	z_3	z_{11}	z_{15}	1	z_1	z_{10}	z_6	z_4

The result is

$$3(8,1)+4(8,3)+8=-(8,1)+4.$$

Thus

$$(8,1)^2+(8,1)-4=0$$

and

$$(8,1)=\frac{-1\pm\sqrt{17}}{2}.$$

To decide which sign to take, we calculate both sides approximately. The left side is 1.56155. With the positive sign the right side gives the same approximation. Thus

$$(8,1)=\frac{-1+\sqrt{17}}{2}$$

$$z_9\times z_{13}=z_{22}=z_5\quad z_9^9\times z_1^{13}=z_1^{22}=z_1^5.$$

The next step is to look at those elements that are not changed by σ^4. These are all of the form:

$$a(4,1)+b(4,3)+c(4,9)+d(4,10).$$

Here

$$\begin{aligned}(4,1)&=z_1+z_{13}+z_{16}+z_4\\(4,3)&=z_3+z_5+z_{14}+z_{12}\\(4,9)&=z_9+z_{15}+z_8+z_2=(8,1)-(4,1)\\(4,10)&=z_{10}+z_{11}+z_7+z_6\end{aligned}$$

I could calculate both $(4,1)\times(4,1)$ and $(4,1)\times(4,9)$. The point is that every number that is fixed by σ^4 will be of the form

$$a(4,1)+b(4,3)+c(4,9)+d(4,10).$$

The four basic numbers of this form are $(4,1)$, $(8,1)$,

$$1=-(8,1)-(8,3)$$

and $(4,1)\times(8,1)$. Since $(4,1)^2$ must also be a number of this form, we will have

$$(4,1)^2=a(4,1)+b,$$

with $a=c(8,1)+d$, $b=e(8,1)+f$, so that a and b are numbers that we know we can construct with ruler and compass. Since

$$(4,1)=\frac{a\pm\sqrt{a^2+4b}}{2},$$

it too can be constructed.

A simpler way to proceed is to observe that $(4,1)$ and $(4,9)$ satisfy the equation

$$0 = \big(Z-(4,1)\big)\big(Z-(4,9)\big) = Z^2 - \big((4,1)+(4,9)\big)Z + (4,1)(4,9)$$

which equals

$$Z^2 - (8,1)Z + (4,1)(4,9).$$

Using this, it is enough to calculate $(4,1)(4,9)$ in which there are only sixteen terms.

	z_1	z_{13}	z_{16}	z_4
z_9	z_{10}	z_5	z_8	z_{13}
z_{15}	z_{16}	z_3	z_6	z_{11}
z_8	z_9	z_4	z_7	z_{12}
z_2	z_3	z_{15}	z_1	z_6

The sum of all these numbers is -1. Thus

$$(4,1)^2 - (8,1)(4,1) - 1 = 0$$

and

$$(4,1) = \frac{(8,1) \pm \sqrt{(8,1)^2+4}}{2}.$$

Since $(8,1)^2 = -(8,1)+4$, the expression under the square root is $8-(8,1)$. We find that

$$\frac{(8,1)+\sqrt{8-(8,1)}}{2} = \frac{\frac{-1+\sqrt{17}}{2} + \sqrt{\frac{17-\sqrt{17}}{2}}}{2} \sim 2.04948 \sim (4,1)$$

and this determines the sign.

Notice that

$$\frac{(8,1)-\sqrt{8-(8,1)}}{2} \sim -0.487928.$$

So there is no ambiguity!

The next step is to find an expression for the period

$$(2,1) = z_1 + z_{16}$$

invariant under σ^8.

We consider also

$$(2,13) = z_{13} + z_4$$

because $(2,1)+(2,13) = (4,1)$. Thus with any luck, we can calculate $(2,1)$ if we can calculate $(2,1)\times(2,13)$. It is given by the table

	z_1	z_{16}
z_{13}	z_{14}	z_{12}
z_4	z_5	z_3

This gives $(4,3)$, which we have not yet calculated. There are two possibilities: to express $(4,3)$ as $a(4,1)+b$ with $a = c(8,1)+d$, $b = e(8,1)+f$, where c, d, e, f are ordinary fractions, or to calculate $(4,3)$ as we calculated $(4,1)$. The second method is easier.

First of all,

$$(4,3)+(4,10) = (8,3) = \frac{-1-\sqrt{17}}{2}.$$

We calculate $(4,3) \times (4,10)$ in the usual way:

	z_3	z_5	z_{14}	z_{12}
z_{10}	z_{13}	z_{15}	z_7	z_5
z_{11}	z_{14}	z_{16}	z_8	z_6
z_7	z_{10}	z_{12}	z_4	z_2
z_6	z_9	z_{11}	z_3	z_1

The sum is -1, so that

$$(4,3)^2 - (8,3)(4,3) - 1 = 0.$$

Thus

$$(4,3) = \frac{(8,3) \pm \sqrt{(8,3)^2 + 4}}{2} = \frac{(8,3) \pm \sqrt{8 - (8,3)}}{2},$$

so that the expression for $(4,3)$ is exactly the same as that for $(4,1)$, except that $(8,3)$ replaces $(8,1)$.

$$(4,3) = \frac{(8,3) \pm \sqrt{(8,3)^2 + 4}}{2}.$$

We still have to check the sign numerically. It is positive.

$$(4,3) \sim 0.344151 \sim \frac{(8,3) + \sqrt{8 - (8,3)}}{2}$$

Thus

$$(4,3) = \frac{\frac{-1-\sqrt{17}}{2} + \sqrt{\frac{17+\sqrt{17}}{2}}}{2}.$$

We return to $(2,1)$, which we know satisfies the equation

$$Z^2 - (4,1)Z + (4,3) = 0.$$

Thus

$$(2,1) = \frac{(4,1) + \sqrt{(4,1)^2 - 4(4,3)}}{2}.$$

The expression under the square-root sign is

$$\left(\frac{\frac{-1+\sqrt{17}}{2} + \sqrt{\frac{17-\sqrt{17}}{2}}}{2} \right)^2 - 4 \left(\frac{\frac{-1-\sqrt{17}}{2} + \sqrt{\frac{17+\sqrt{17}}{2}}}{2} \right).$$

Since

$$\left(\frac{-1 + \sqrt{17}}{2} \right)^2 = \frac{9 - \sqrt{17}}{2},$$

the first square is equal to

$$\frac{13 - \sqrt{17}}{4} + \frac{(-1 + \sqrt{17})\sqrt{\frac{17-\sqrt{17}}{2}}}{4}.$$

All together, we have

$$\frac{17 + 3\sqrt{17}}{4} + \frac{(-1 + \sqrt{17})\sqrt{\frac{17-\sqrt{17}}{2}}}{4} - 2\sqrt{\frac{17 + \sqrt{17}}{2}}.$$

Since

$$\frac{(4,1)}{2} = \frac{-1}{8} + \frac{\sqrt{17}}{8} + \frac{\sqrt{34-2\sqrt{17}}}{8},$$

we find that $(2,1)$ is equal to

$$\frac{-1}{8} + \frac{\sqrt{17}}{8} + \frac{\sqrt{34-2\sqrt{17}}}{8} \pm \frac{\sqrt{68+12\sqrt{17}-16\sqrt{34+2\sqrt{17}}-2(1-\sqrt{17})\sqrt{34-2\sqrt{17}}}}{8}.$$

This is the form to be found in Klein's lectures.

Of course the sign has to be discovered by numerical approximation. We find that, with the plus sign both $(2,1)$ and this expression are about 1.86494.

Gauss's form is

$$\frac{-1}{8} + \frac{\sqrt{17}}{8} + \frac{\sqrt{34-2\sqrt{17}}}{8} + \frac{\sqrt{68+12\sqrt{17}-8\sqrt{34+2\sqrt{17}}-4\sqrt{34-2\sqrt{17}}}}{8}.$$

It is obtained from Klein's by means of the square root of the identity

$$16(34+2\sqrt{17}) = (18+2\sqrt{17})(34-2\sqrt{17}) = (1+\sqrt{17})^2(34-2\sqrt{17}).$$

This means

$$16\times 34 = 18\times 34 - 4\times 17 \qquad 16\times 2 = 2\times 34 - 18\times 2.$$

We have now established that $(2,1) = z_1 + z_{16}$ can be found by repeatedly extracting roots. Recall that

$$z_1 = \cos(2\pi/17) + i\sin(2\pi/17)$$

and that

$$z_{16} = \cos(32\pi/17) + i\sin(32\pi/17) = \cos(2\pi/17) - i\sin(2\pi/17).$$

Thus

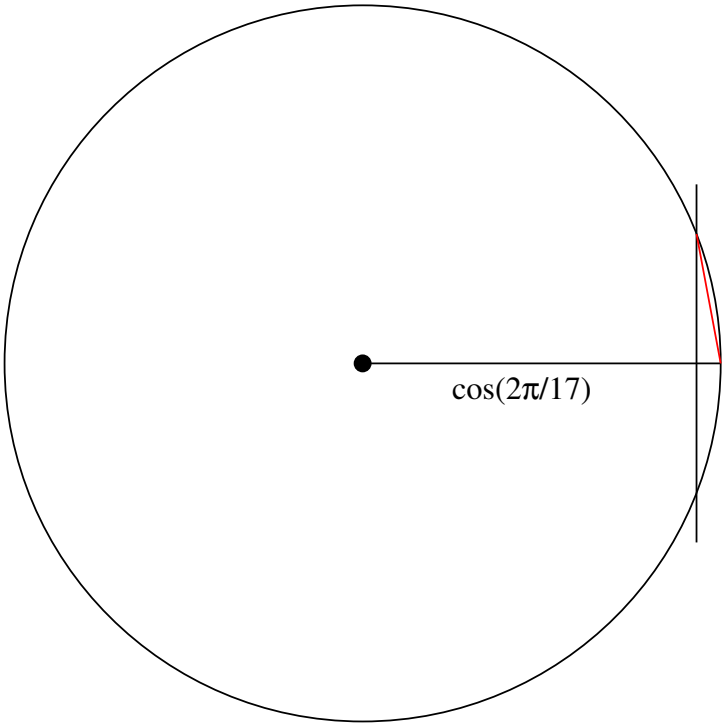
$$(2,1) = 2\cos(2\pi/17),$$

so that $\cos(2\pi/17)$ can be found by repeatedly extracting square roots. Since z_1 is a root of

$$0 = (Z-z_1)(Z-z_{16}) = Z^2 - (2,1)Z + 1,$$

it can be found by extracting one more square root.

Of course, once $a = \cos(2\pi/17)$ is found, the usual way to construct z_1 is by erecting a perpendicular to the axis of abscissas at $(a,0)$ and intersecting it with the circle $x^2+y^2=1$.


cos(2π/17)

Final remark

The algebraic analysis shows how we are to proceed geometrically to construct successively the following numbers:

1) (8,1) and (8,3);
2) (4,1) and (4,3);
3) (2,1).

The numbers at each stage are obtained from those at the preceding stage by solving a quadratic equation—thus in effect by extracting a square root. Once we show how to solve in general a quadratic equation with given coefficients, we can proceed efficiently step by step. This is done in Klein's *Famous problems of elementary geometry*. It is clearly best to take the steps one at a time and not to represent them all together, but time is brief. So I present them to you all together as Klein finally does, although he also gives each step as well as describing an efficient way for solving a quadratic equation with known coefficients.

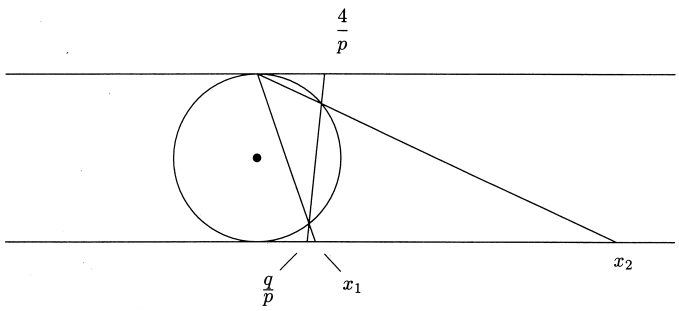
In addition to Klein, you might want to consult a text in a recent issue of the *Mathematical Intelligencer* that Robert Feinberg drew to my attention. It can be found in the mathematics library and in the common room in the mathematics building.

> Christian Gottlieb, *The simple and straightforward construction of the* 257*-gon*, Math. Int., vol. 21, No. 1, 1999.

Observe that 257 is a prime and that

$$257 - 1 = 256 = 16^2 = 2^8 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2,$$

so that eight steps are required and not just four to arrive at the final result. In addition, the individual calculations will be longer as will the final formulas.



$$x^2 - px + q = 0$$

THE REGULAR POLYGON OF 17 SIDES. 41

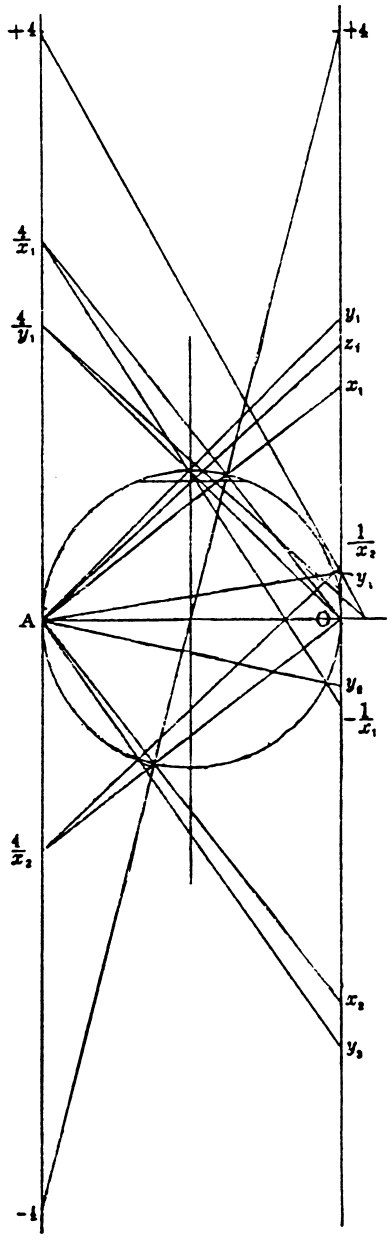


FIG. 9.

Lecture 1 [Lecture 9]

Introduction

My announced intention was to reach a stage where I could introduce ideal numbers, which are then divided into classes, and could then describe the relation between the problem of counting these classes and the zeta function of Riemann. In one way or another almost all the outstanding problems of modern number theory, and there are a tremendous number of them, are part of a program to use analytical methods to evaluate numbers of various kinds that characterize the size of objects, such as the classes of ideal numbers, that arise in the analysis of diophantine equations, thus equations with integral or rational coefficients for which integral or rational solutions are wanted. These analytical methods are methods that can be easily implemented on a computer and in which there is no uncertainty, no possibility of embarking on an endless search for numbers that may or may not exist, as might happen if one undertook a direct search for solutions of such an equation.

The zeta function will probably be given short shrift, not because it cannot be introduced at the same level as the other material, but because there is not enough time in the eight lectures to treat everything. So the zeta function will be replaced by a pale reflection, the Bernoulli numbers.

The ideal numbers and their division into classes were introduced by Kummer during his attempt to prove the Fermat theorem, as was the relation between the number of classes and the Bernoulli numbers, easily calculated rational numbers. Kummer's success with Fermat's theorem was limited, but he took the subject a long way. Moreover his notion of ideal number and in general his investigation of complex numbers constructed, in a manner now familiar to us, from the solutions of equations in one variable with rational coefficients, was one of two principal starting points, the other being the analysis of symmetries associated to the name of Galois, for the development during the rest of the nineteenth century and the course of the twentieth of the theory of algebraic numbers, without which, I stress, Fermat's theorem could not have been solved, and of which indeed the recent proof has to be regarded as a part.

As preparation for Kummer, we shall spend a considerable amount of time with the work done on Fermat's theorem by Euler and others, between 1750 and 1840.

Puzzlement

Before dealing with ideal numbers, especially ideal primes, we had best provide ourselves with the basic notion of ordinary primes and their uses. Since these are treated by Euclid in Book VII—indeed the basic technique, the euclidean algorithm,

Date of lecture: Spring term, February 1, 2000.

is given there—it seemed to the point to continue the procedure of the fall lectures, and to begin with Euclid. This I shall do, even though Euclid's treatment of everything but the basic algorithm is fundamentally different from the modern treatment.

I find Book VII in general puzzling, as I shall explain in the course of presenting some of the propositions. What seems to me the enunciation of the basic proposition (Proposition 4) to be deduced from the algorithm is obscurely formulated and its proof even more badly explained. Almost all of the succeeding propositions, many of which we shall need, are almost immediate consequences of Proposition 4, but this is not clearly explained. If this were a modern book, I would be tempted to suggest that the author did not understand the material, but it is a book with the patina of more than two millennia, so that this would be impertinent.

I had hoped to find some enlightenment in Heath's comments, which presumably reflect the state of historical research in 1925. I was disappointed. In contrast to his commentary on the earlier books, that on Book VII is perfunctory, consisting largely of translations of the statements into modern notation and language.

It may be that the clue to the obscurity is that Euclid was translating essentially arithmetical arguments, thus the kind of arguments that might have been preferred in earlier, Pythagorean times into the geometric arguments preferred after the crisis created by the discovery of the irrational, but I do not know. I have searched the literature, although not thoroughly, and made inquiries of specialists, but so far have found very little that is pertinent.

The search is, however, not without its amusing aspects. There is an article—presumably written by a historian of mathematics with no pretensions as a professional mathematician—in which elderly mathematicians who have taken up the history of their subject are upbraided for their Whiggish tendencies and in which it is insinuated that their excursions (or incursions) into this foreign territory are little more than embarrassingly public confessions of the mathematical impotence reputed to appear among us with advancing age and there is a response from one of these same elderly mathematicians, impotent or not, who, with a childish or primitive belief that denying someone his name also robs him of his dignity, castigates an anonymous but clearly identified Z, who is left to infer on his own, although he is guided carefully through each step of the exercise, that he is a "would-be historian" and a "parasite".

Instructive as such articles, in their own way, are, they do not suggest that the study of Euclid since the time of Heath has made great strides, but I continue to look.

There is, however, a remark of the professional historian (S. Unguru) that I would like to cite, as it is possible that it is a clue to the puzzling form of Book VII.

> *It seems to me that it is a considerably more appealing (and certainly historically more defensible) thesis that Greek mathematics, as found in the* Elements*, is an outgrowth of* PYTHAGOREAN *mathematics, the arithmetical discreteness of the former (with all its accompanying inherent weaknesses) having been replaced in the former by the continuity of geometrical magnitude; thus in* EUCLID *numbers are not collections of points anymore, but segments of straight lines,* etc.

Even before seeing this remark, I had decided that the propositions of Book VII and their proofs would be much easier to follow if I replaced the line segments of Euclid by points, and I have done so. Thus I have changed the accompanying figures without changing the arguments. I observe that I cannot judge to what extent the figures appearing in Euclid are a response to the initial medium or to what extent they are Euclid's own, and not those of subsequent editors.

In contrast to the historian's suggestion, a statement by the professional mathematician (A. Weil) appears to be questionable.

> *In* EUCLID*'s books* VII, VIII *and* IX *there is no trace of geometry, nor even of so-called 'geometrical algebra'.*

If the geometric traces, namely the line segments, are entirely factitious, a result of self-imposed logical or pedagogical constraints, and therefore to be disregarded—a doubtful historical procedure—then the two statements can be reconciled.

Further comments

On further reflection there is a possible explanation for the uneasiness felt on reading Book VII. Implicit in the argument, as presented by me or by Euclid, is the assumption that counting the number of units we always arrive at the same result. For us, with an *a priori* notion of number, for example, to be less than precise mathematically, of the number 8 as a linearly ordered set of eight points, there is something to be proved: it must be proved that two different ways of counting a given collection (or *multitude* in the language of Heath's Euclid) always leads to the same result. This is proved explicitly in texts on set theory.

On the other hand, it is only implicit in Euclid's Book VII. If we return to the very beginning of Book I, we find two of the *common notions* affirming that the whole is greater than the part and that equals subtracted from equals yield equals. Geometrically, this would mean, for example, that removing a unit length from the middle of a longer length and splicing the two remaining ends leads to a length that is the same as if we had simply snipped the unit length from one end. This principle when elaborated could remove the vagueness that appears in Euclid's notion of number—to which we shall come immediately.

It may have been that Euclid, and other Greek mathematicians, had more confidence in the immutability of length than in the immutability of a more abstract notion of number. Indeed as we have already seen, their confidence in the notion of area allowed them to use it in their arguments with a freedom that modern mathematicians felt obliged to justify with the help of their own, recently introduced, notions of number. For example, a modern mathematician is compelled to show that not all numbers are equal.

Comment

Despite strictures about the flaws of Whig history, the principal purpose for which a mathematician pursues the history of his subject is inevitably to acquire a fresh perception of the basic themes, as direct and immediate as possible, freed of the overlay of succeeding elaborations, of the original insights as well as an understanding of the source of the original difficulties. His notion of basic will certainly reflect his own, and therefore contemporary, concerns. For the period that begins with Fermat and ends just before Kummer, there is, so far as I know, no

better treatment than that of the elderly mathematician André Weil, whom I have just cited in a more polemical mood. The pertinent book is

Number Theory—An approach through history.

I recommend it to you.

For the early Greek theorems about numbers, there seems to be no adequate reference.

Euclid: Book VII

Some Definitions.

1. A **unit** is that by virtue of which each of the things that exist is called one.
2. A **number** is a multitude composed of units.
3. A number is a **part** of a number, the less of the greater, when it measures the greater;
4. but **parts** when it does not measure it.
5. The greater number is a **multiple** of the less when it is measured by the less.
11. A **prime number** is that which is measured by a unit alone.
12. Numbers **prime to another** are those which are measured by a unit alone as a common measure.
13. A **composite number** is that which is measured by some number.
14. Numbers **composite to one another** are those which are measured by some number as common measure.
15. A number is said to **multiply** a number when that which is multiplied is added to itself as many times as there are units in the other, and thus some number is produced.
20. Numbers are **proportional** when the first is the same multiple, or the same part, or the same parts, of the second that the third is of the fourth.

Observe that for Euclid the unit is not a number, thus there is no number 1. The notion of **parts** is obscure and means more than the definition suggests. This is clear from Definition 20.

Some examples

Primes.

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$$

Composite numbers.

$$4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30$$

Numbers prime to one another.

10 and 21.

Numbers composite to one another.

15 and 27—measured by 3

Since 15 is the multiple 5 of 3, the number 3 is to be thought of as one 5th part of 15. On the other hand 10 is parts of 22 and as we shall see this parts is to be thought of as 5 of 11 parts.

The notion of parts will be explained further when we verify the following proposition.

Proposition VII.4. *Any number is either a part or parts of any number, the less of the greater.*

From the definitions, this proposition seems to say nothing at all. This is not so. It is in fact important, and can only be established after an important technique has been introduced, one that will appear in other contexts.

Five measures fifteen

Euclid's algorithm: first case

Proposition VII.1. *Two unequal numbers being set out, and the less being continually subtracted in turn from the greater, if the number which is left never measures the one before it until a unit is left, the original numbers will be prime to one another.*

An example. Take the numbers 22 and 105. Then

$$\begin{array}{ccc} 105-22=83 & 83-22=61 & 61-22=39 \\ 39-22=17 & 22-17=5 & 17-5=12 \\ 12-5=7 & 7-5=2 & 5-2=3 \\ 3-2=1. & & \end{array}$$

Another example. Take 35 and 10. Then

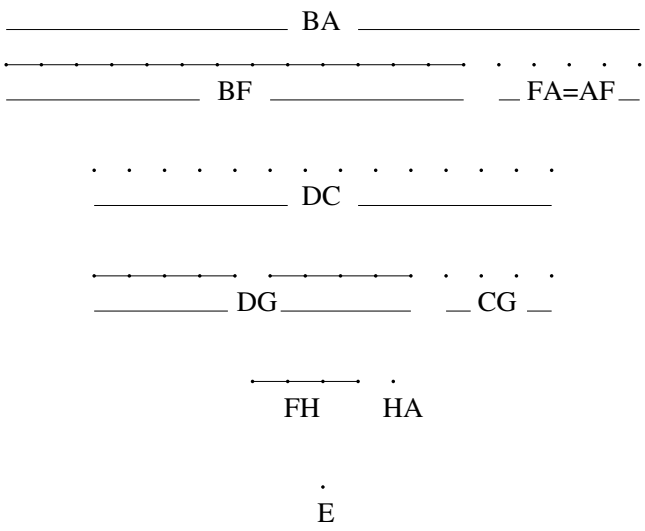
$$35-10=25 \qquad 25-10=15 \qquad 15-10=5$$

and 5 measures 10.

Proof

We prove the proposition with Euclid's notation. Take the two numbers to be AB and CD. Suppose that they are not prime to one another. Then they are measured by E. If for example, CD is less than AB, subtract CD continually from AB, obtaining BF which is measured by CD and a remainder FA which is less than CD. Let then AF measure GD leaving CG which is less than itself. Then let GC measure FH leaving HA. Since E measures CD and CD measures BF, therefore E also measures BF. But it measures the whole BA. Therefore it also measures AF. But AF measures DG, so that E also measures DG. Since it also measures DC, it measures CG. But CG measures FH, so that E also measures FH. Since it also measures FA, it measures the unit AH. This is impossible.

Proposition 1



Second case

Proposition VII.2. *Given two numbers not prime to one another, to find their greatest common measure.*

We repeat the previous process. If the smaller of the two CD measures AB, then it is the greatest common measure. Otherwise, we repeatedly subtract CD from AB until we have found EB measured by CD and a remainder AE smaller than CD. It will not be the unit, because AB and CD are not prime to one another. Either this remainder AE measures CD and therefore also AB or it does not and it will measure FD leaving the remainder CF smaller than itself, which will again not be a unit. If CF measures AE, then it measures FD and also CD, and therefore also AB. Thus it will be a common measure of AB and CD.

It is also the greatest. If not let G be a number greater than CF that measures both AB and CD. Then G measures both BE and AB so that it measures AE. Continuing, we see that it measures CD and FE, so that it also measures CF. Since it was supposed greater than CF, this is impossible.

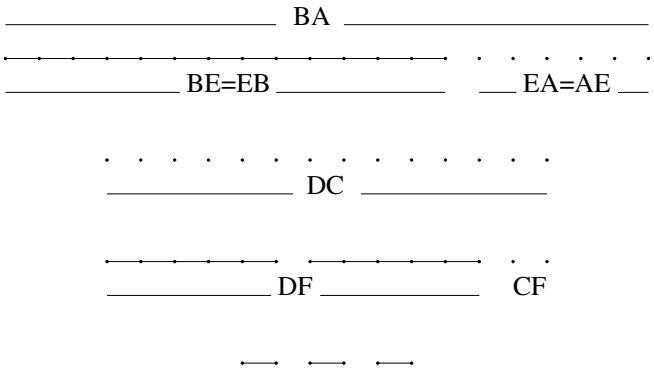
A consequence of the algorithm drawn by Euclid

Proposition VII.30. *If two numbers by multiplying one another make some number, and any prime number measure the product, it will also measure one of the original numbers.*

This proposition, stated in modern notation, means that if the prime number p divides ab then it divides either a or b, supposed of course to be integers. In conjunction with the following, easy proposition, it implies that every positive integer is the product, in a unique way up to order, of primes, although this fact does not appear in Euclid, who does not explicitly mention such a possibility, perhaps because he is not inclined to consider the product of several numbers.

Proposition VII.32. *Any number either is prime or is measured by some prime number.*

Proposition 2



Two measures six

A modern consequence

Granted the two propositions we start from a positive number n. It is either prime, and then $n = p$ or it is divisible by a prime p and then $n = pm$. Continuing with m, we continually divide by a prime, the quotient growing smaller and smaller, until it is 1. The uniqueness follows because, as a result of Proposition 30, if p divides abc then it divides one of $a, b, c, \ldots$. Thus if

$$p_1^{a_1} \cdots p_k^{a_k} = q_1^{b_1} \cdots q_\ell^{b_\ell},$$

with all of $a_1, \ldots$ and $b_1, \ldots$ positive, then p_1 is one of $q_1, q_2, \ldots$. So we divide both sides, one by p_1 and one by $q_j = p_1$ and continue with at least one a_i and at least one b_j smaller. Arriving finally at an expression in which one side is 1, and therefore in which both sides are 1.

Observe that this is a direct consequence of Proposition 30. Presumably it was not drawn by Euclid because he had no way of expressing the product of large numbers of integers, or even of more than three integers.

In a modern treatment, the unit would be an integer, so that Propositions 1 and 2 would be formulated as a single proposition, somewhat differently stated, from which Proposition 30 would follow directly. In Euclid this is not so and there are a large number of propositions in Book VII between the first two and the thirtieth. Their purpose is, so far as I can see, largely to explain the notion of greatest common measure, a notion which for us has become, by the time we come to discuss primes, completely intuitive. I begin by discussing Proposition VII.4.

In other words, as so often with Euclid, the difficulty does not lie in the proof of Proposition 30. It lies elsewhere, in earlier propositions, where the meaning of **part** and of **parts** is explained and connected with the notion of ratio. Proposition 32 is pretty much a direct consequence of the definitions.

An immediate consequence drawn by Euclid

This is the unicity of the greatest common measure. Euclid's conclusion is formulated as a porism.

Porism. *From this it is manifest that, if a number measure two numbers, it will also measure their greatest common measure.*

Explanation and proof of proposition VII.4

I use Euclid's notation. Let A and BC be two numbers and let BC be the less. He unfortunately distinguishes the case that A and BC are prime to each other from the case that they are not.

If they are prime to one another, then if BC is divided into the units in it, each unit of those in BC will be a part of A, so that BC is parts of A. In other words, A is a certain number of units; and CD is some smaller number of those units, and therefore makes up a proper fraction of the total number of units in A.

If they are not prime to one another, then either BC measures A and is therefore a part of A (In modern terminology, BC over A is a fraction $1/n$ with numerator 1) or BC does not measure A and there is a greatest common measure D that can be found by Proposition 2. Then D measures BC, so that BC can be divided into numbers BE, EF, FC equal to D.

Interpolation. *Thus BC is made up of several pieces, say m of size D.*

As D measures A, D is a part of A.

Interpolation. *Thus A is made up of several pieces of size D, say n. Moreover m is less than n. We conclude that m of those n parts makes CD* ***parts*** *of A.*

Euclid's version: But D is equal to each of the numbers BE, EF, FC; therefore each of the numbers BE, EF, FC is also a part of A; so that BC is part of A.

What this proposition says is that, using the Euclidean algorithm, we can find two integers, m and n, necessarily prime to one another such that $BC : A = m : n$, but this appears to be very difficult for Euclid to articulate. Notice that if BC measures A then $m = 1$.

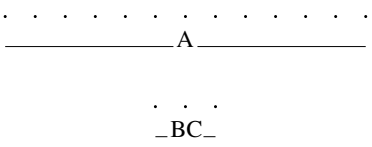
Notice also that we can break BC up into m parts all equal to each other and to each of the n parts into which we break up A.

This pair of numbers m and n is what defines the **part** or **parts** of the pair BC and A and Definition 20 makes two pairs proportional if they have the same parts.

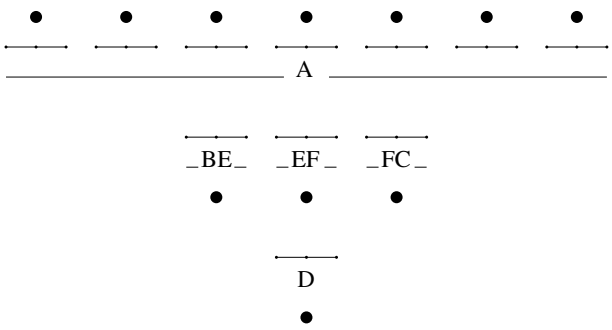
With this proposition in hand, I am going to give some consequences, using the arguments of Euclid and formulating the conclusions as propositions following him. Since the language of these propositions is, however, obscure, preference will be given to clear formulations in everyday language.

Proposition 4

Example 1.



Example 2.



Further propositions

The first thing to observe is that if $A : B = C : D$ in the sense of Definition 20, then $A : C = B : D$. The first equality means that we can divide A and B into n and m parts respectively of equal size E and then C and D into the same numbers n and m of another size F. Then we apply Proposition VII.4 to the pair E and F, dividing them into pieces of equal (integral!) size k and ℓ. It is clear then that the part or parts of the pair A and C is k/ℓ as is that of the pair B and D.

This fact is expressed by Euclid as Proposition VII.13.

Proposition 13. *If four numbers be proportional, they will also be proportional alternately.*

He also shows that if A, B and C are numbers, then

$$B : C = AB : AC.$$

He formulates this as two propositions.

Proposition 17. *If a number by multiplying two numbers make certain numbers, the numbers so produced will have the same ratio as the numbers multiplied.*

Proposition 18. *If two numbers by multiplying any number make certain numbers, the numbers so produced will have the same ratio as the multipliers.*

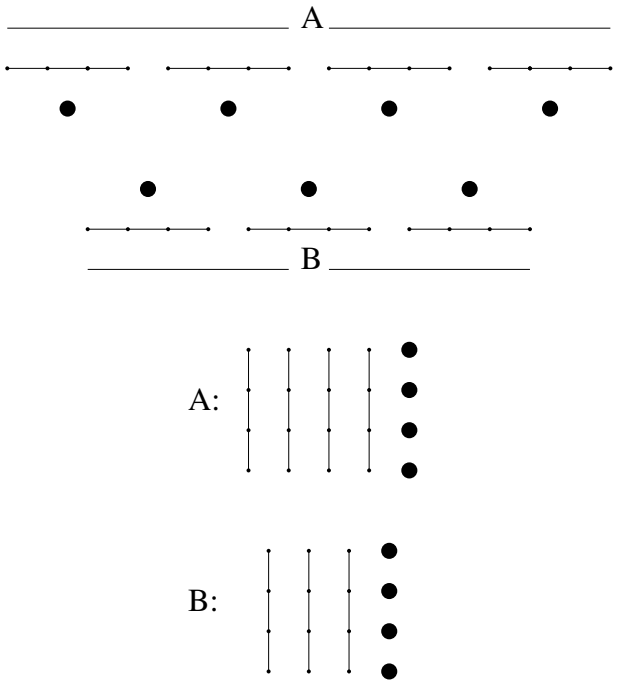
I observe that he proves these propositions separately, even though he has just proved that multiplication is commutative. Thus there is some redundancy. The proof is best presented as a diagram.

He also shows that $A : B = C : D$ in the sense of Definition 20 if and only if $AD = BC$. Here is the relevant proposition.

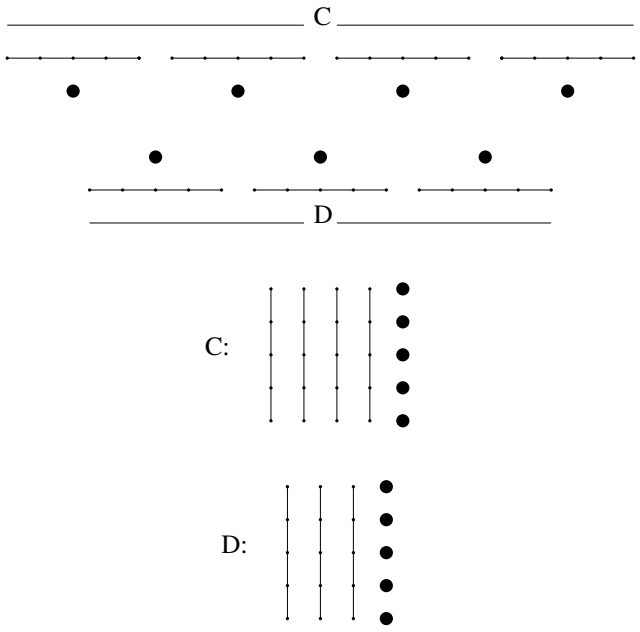
Proposition 19. *If four numbers be proportional, the number produced from the first and the fourth will be equal to the number produced from the second and the third; and if the number produced from the first and the fourth be equal to that produced from the second and the third, the four numbers will be proportional.*

To prove the first part of the proposition, let A, B, C and D be the numbers in proportion. Let A multiplying D make E and let B multiplying C be F. Finally let A multiplying C make G. Represent these three numbers and the relation $A : B = C : D$ as in the diagrams. The conclusion follows, as does the second half of the proposition.

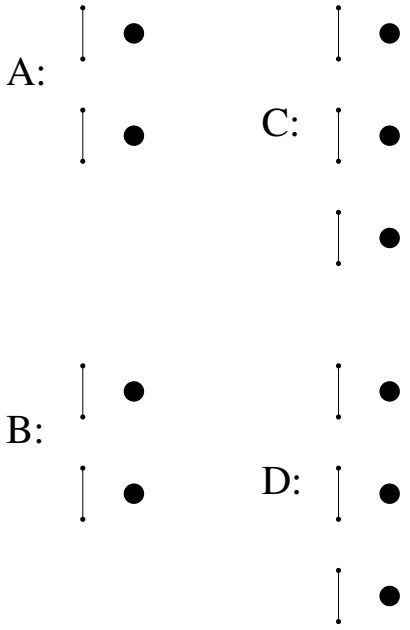
Proposition 13



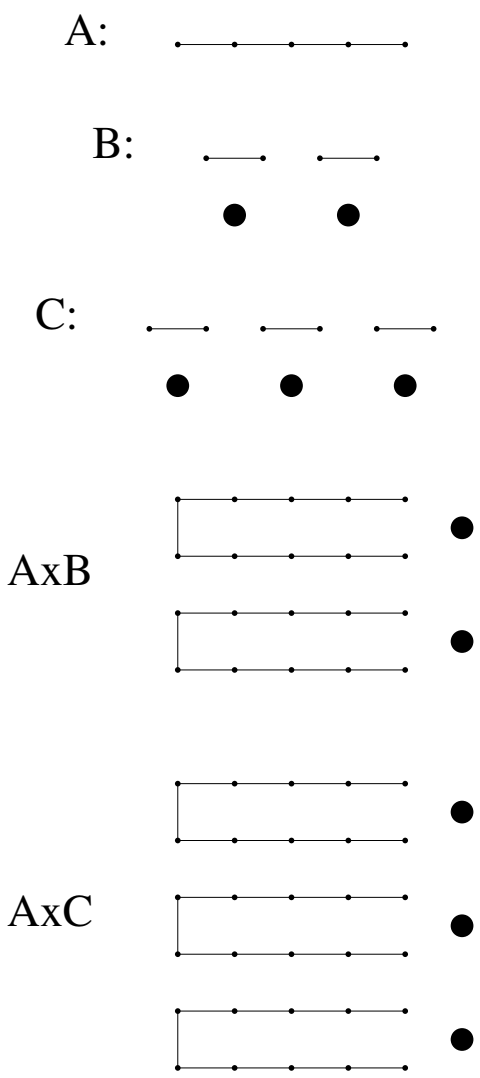
Proposition 13: continued



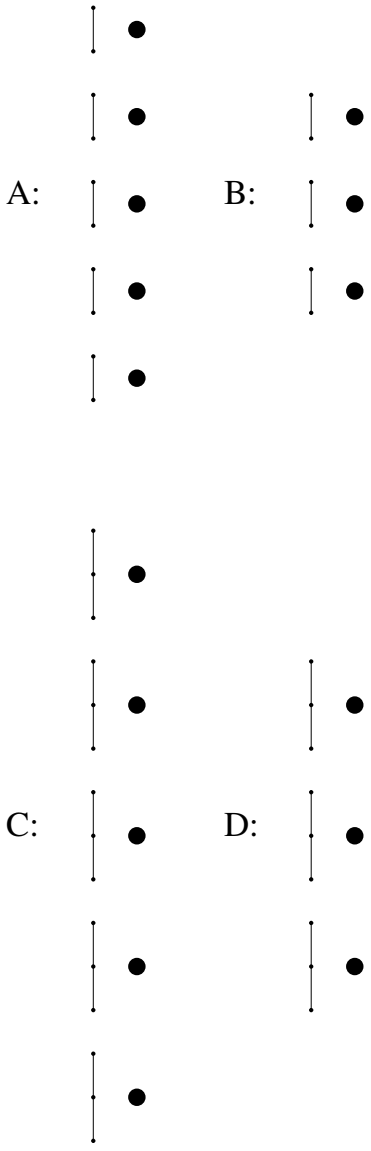
Proposition 13: a possible final step



Proposition 17

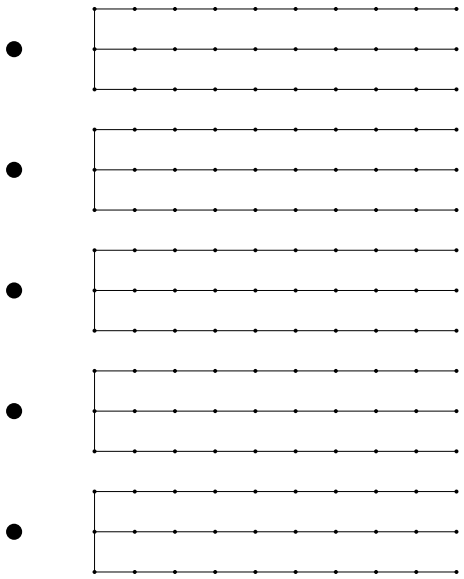


Proposition 19: first half

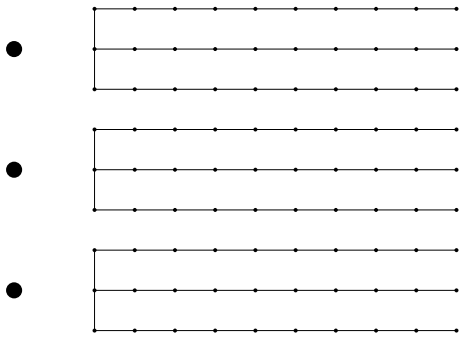


Proposition 19: first half continued.

The number produced from A and C:

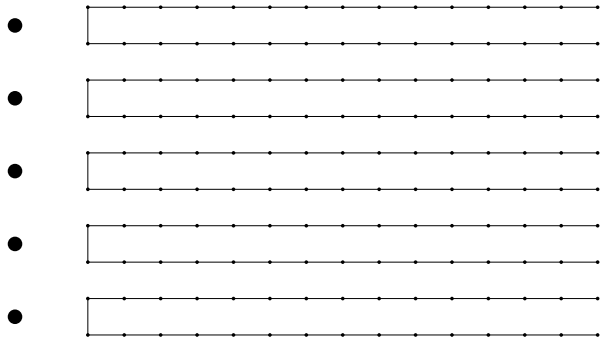


The number produced from A and D:

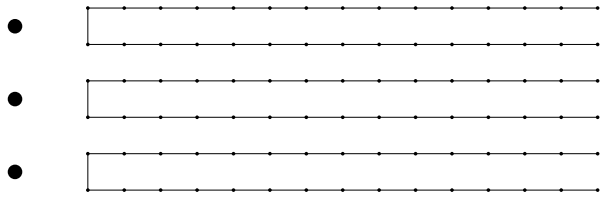


Proposition 19: first half completed.

The number produced from A and C:



The number produced from B and C:



Lecture 2 (and Lecture 4) [Lecture 10 (and Lecture 12)]

Further propositions: continued

The next proposition is a matter of putting a fraction in least common terms, but that has already been done in Proposition 4, so that this should be pretty much a repeat.

Proposition 20. *The least numbers of those which have the same ratio with them measure those which have the same ratio the same number of times, the greater the greater and the less the less.*

What this means is that if $A : B$ is equal to $CD : EF$ and if CD or, what is the same if (and only if) one thinks about it, if EF is as small as possible, then A is a multiple of CD and B the same multiple of EF. It seems to me that CD and EF must obviously be the pair of integers discovered while proving Proposition 4. So the proof of Euclid appears to me unnecessary.

Proposition 21. *Numbers prime to one another are the least of those which have the same ratio with them.*

This too seems a consequence of the proof of Proposition 4.

Proofs of propositions 30 and 32

It seems to me that this Proposition 32 is pretty much a consequence of the definitions. If a number A is prime, there is nothing to be done. Otherwise it is measured by a smaller number B, If B is prime, there is nothing further to be done. Otherwise it is measured by an even smaller C. Continuing in this way, we arrive finally at a prime.

To establish Proposition 30 following Euclid is another matter. We let A and B be two numbers and multiplying them together we obtain C. Suppose that D is a prime number that measures C. If D does not measure A then A and D are prime to each other. Suppose C is obtained by multiplying D and E. Thus

$$A \times B = D \times E$$

so that

$$A : D = E : B$$

Since A and D are prime to each other, they are the least of the numbers that have the same ratio as they do. Thus they measure E and B respectively. In particular, D measures B.

Date of lecture: Spring term, February 8 (and 22), 2000.

Illustration of proposition 32

Consider the number 10,780. It is not prime as it is divisible by 10. Dividing by 10, we obtain 1,078, which is not prime as it is divisible by 2. Dividing by 2, we obtain 539, which is divisible by 7. To be precise $539 = 7 \times 77$. Finally 77 is divisible by either 7 or 11, both of which are primes.

A modern treatment

The unique factorization of numbers into primes will be so important to us, either as a fact or as a model, that a complete understanding of it and its proof is an essential prerequisite for all that follows. Since Euclid's treatment is much less transparent than the modern, and indeed—apart from the basic algorithm—is quite different in spirit from the modern understanding, I review quickly the modern treatment—in a modern notation.

Suppose a and b are two natural numbers, thus 1, 2, 3 and so on, where in contrast to Euclid, I have included the unit 1 as a number. This is just to avoid repetition. Consider the collection M of all the numbers m that can be represented as $ka + \ell b$, where k and ℓ are integers that may not be positive. If a is larger than b and we replace a by $a - b$, then

$$m = ka + \ell b = k(a - b) + (\ell + k)b = ka' + \ell' b.$$

Thus subtracting b from a to obtain a' does not change the collection M. It just changes the representation of a given m. We can repeatedly subtract b until we arrive at $c = a - nb$ that is smaller than b. If it is 0 then $a = nb$ and $m = ka + \ell b = (kn + \ell)b$ is a multiple of b. Thus M consists exactly of the multiples of b. In particular a is a multiple of b and b is the greatest common measure (called nowadays **divisor** of a and b). Otherwise we replace a by c and the pair $\{a, b\}$ by $\{b, c\}$. This does not change M. We next subtract the largest possible multiple of c from b to obtain d. If this result is 0 then M consists of multiples of c and c is the greatest common divisor of a and b because it divides a and b, both of which lie in M, and is itself in M. Notice that any number that divides both a and b divides every number in M. If d is not 0 we replace $\{b, c\}$ by $\{c, d\}$. Once again this does not change m. Since d is smaller than c, and at each stage the second element of the pair grows smaller, it must eventually be 0 and the second element at the preceding stage will be the greatest common divisor of a and b.

Table of $15k + 21\ell$**,** $k = -5, \ldots, 5$**,** $\ell = -4, \ldots, 4$

$k\backslash\ell,$	-4	-3	-2	-1	0	1	2	3	4
-5	-159	-138	-117	-96	-75	-54	-33	-12	9
-4	-144	-123	-102	-81	-60	-39	-18	3	24
-3	-129	-108	-87	-66	-45	-24	-3	18	396
-2	-114	-93	-72	-51	-30	-9	12	33	54
-1	-99	-78	-57	-36	-15	6	27	48	69
0	-84	-63	-42	-21	0	21	42	63	84
1	-69	-48	-27	-6	15	36	57	78	99
2	-54	-33	-12	9	30	51	72	93	114
3	-39	-18	3	24	45	66	87	108	129
4	-24	-3	18	39	60	81	102	123	144
5	-9	12	33	54	75	96	117	138	159

A modern treatment: continued

Example.

$$a = 147, \quad b = 27.$$

$$147 - 5 \times 27 = 147 - 135 = 12,$$
$$27 - 2 \times 12 = 27 - 24 = 3,$$
$$12 - 4 \times 3 = 12 - 12 = 0$$

Thus the greatest common divisor of 27 and 147 is 3.

In particular, if a and b are prime to one another or, in modern terminology, relatively prime, then there are integers k and ℓ such that $ka + \ell b = 1$. Conversely, if there are such integers k and ℓ, then a and b are relatively prime.

We return to Proposition 30. Suppose then that a and b are both relatively prime to the number d and $c = ab$. Then there are integers k and ℓ such that $ka + \ell d = 1$ and integers m and n such that $mb + nd = 1$. Then

$$1 = (ka + \ell d)(mb + nd) = (km)(ab) + (kan + \ell mb + \ell nd)d = k'c + \ell' d,$$

so that c and d are also relatively prime. If d is a prime number, this is Proposition 30.

Another proposition from Euclid

The next proposition is not one that will be necessary to the logical development of our arguments at first, but it is a very important fact, at the origin of the greatest of all problems in pure mathematics, the Riemann hypothesis and at the core of many other developments in modern mathematics that I would like, sometime, to broach. So, as it is found in Euclid, it is worth a few minutes explaining it, before we pass on to more modern material. Euclid's argument remains one of the modern arguments, the simplest. Notice that the proposition appears in Book IX and not in Book VII.

Proposition IX.20. *Prime numbers are more than any assigned multitude of prime numbers.*

Let (for example) A, B, C be the assigned prime numbers. Let the least prime number measured by A, B and C be DE and let the unit DF be added to DE. (One could also take DE to be the product of A, B and C.) Then EF is either prime or it is not. If it is prime, then the prime numbers A, B, C and EF have been found which are more than A, B, C.

Suppose then EF is not a prime. Let it be measured by the prime number G. G is different than A, B and C. If not, it measures DE because A, B and C measure DE. Thus the remainder of EF on division by G is the unit. But G measures EF. This is absurd. Thus G is not one of A, B and C and the multitude A, B, C and G is more than A, B and C.

Example

The first few primes are 2, 3, 5, 7, 11, 13. Their product is 30,030. Adding 1, we obtain 30,031. It is divisible by the primes 59 and 509.

$$59 \times 509 = 30031.$$

Fermat's theorem: an introduction

I begin by recalling the statement of the theorem.

Fermat's Theorem. *If n is an integer greater than 2 there is no solution of the equation*

$$x^n + y^n = z^n, \qquad xyz \neq 0 \tag{A}$$

in integers.

Recall first that there are solutions if $n = 2$, namely

$$(a^2 - b^2)^2 + (2ab)^2 = (a^2 + b^2)^2,$$

so that we can take $x = a^2 - b^2$, $y = 2ab$, $z = a^2 + b^2$. These are, in essence, the only solutions for $n = 2$, but that is not our concern here.

Recall also that if $n = m\ell$ then

$$(x^\ell)^m + (y^\ell)^m = x^n + y^n = z^n = (z^\ell)^m,$$

so that replacing x by x^ℓ, y by y^ℓ and z by z^ℓ, we obtain from a solution of (A) for n a solution for m. If the impossibility is proved for m it follows also for n. Since every integer greater than 2 is divisible either by an odd prime or by 4, it suffices to prove the impossibility for odd primes and for $n = 4$.

Since 3 is the smallest of these numbers, I start with 3. The key for us will be numbers we have seen before. Let

$$\alpha = \cos(2\pi/3) + i\sin(2\pi/3),$$

so that $\alpha^3 = 1$. We shall study numbers of the form

$$a + b\alpha \tag{B}$$

with a and b integers. These are of course very much like the numbers studied during the discussion of the regular pentagon and regular heptadecagon, except that we then allowed a and b to be fractions, whereas we now want to consider only numbers of this form that are *integral*, at least in a naive sense. It turns out fortunately that this naive sense, which was all that was available at first is equivalent to the more sophisticated and universally correct notion.

OBSERVATIONES DOMINI PETRI DE FERMAT.

I (p. 54).

(Ad definitionem VI Cl. Gasparis Bacheti Porismatum Libr. III.)

A duobus quibuscumque numeris formari dicitur triangulum rectangulum, quum ex aggregato et ex intervallo quadratorum ab ipsis et ex duplo plani sub ipsis numeris contenti constant latera trianguli.

A tribus numeris in proportione arithmetica possumus formare triangulum, si secundum hanc definitionem sextam formemus illud a medio et differentia. Nam solidum sub tribus ductum in differentiam faciet aream dicti trianguli, atque ideo, si differentia sit unitas, solidum sub tribus erit area trianguli.

II (p. 61).

(Ad quæstion. VIII Diophanti Alexandrini Arithmeticorum Libr. II.)

Propositum quadratum dividere in duos quadratos.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duas ejusdem nominis fas est dividere : cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

III (p. 65).

(Ad quæstion. X Libr. II.)

Datum numerum, qui ex duobus componitur quadratis, in alios < duos > quadratos partiri.

Num verò numerum ex duobus cubis compositum dividere poterimus in alios duos cubos? Hæc quæstio difficilis sane nec Bacheto aut Vietæ

The domain $\mathbf{Z}(\alpha)$

Recall that

$$\alpha^2 + \alpha + 1 = 0,$$

so that

$$\alpha = \frac{-1 \pm \sqrt{1-4}}{2}.$$

Since $\sin(2\pi/3) > 0$, $\alpha = (-1 + i\sqrt{3})/2$.

Observe also that

$$(a + b\alpha) \times (c + d\alpha) = ac + (ad + bc)\alpha + bd\alpha^2 = (ac - bd) + (ad + bc - bd)\alpha,$$

so that two numbers of the form (B) when multiplied together yield a number of the form (B). This is also, and clearly, so when they are added or subtracted.

The basis of the proof of Fermat's theorem for $n = 3$ will be the study of primes in the domain of numbers of the form (B). Our first task, will be to prove an analogue of the euclidean algorithm. We begin with a few simple remarks.

First of all the conjugate $\overline{\alpha}$ of α is $\cos(2\pi/3) - i\sin(2\pi/3)$ and $\alpha\overline{\alpha} = 1$. Thus $\alpha^{-1} = \alpha^2$ is $\overline{\alpha}$ and is another number of the same form. The only ordinary integers n such that $1/n$ is also an integer are 1 and -1, but in the new domain, α, $-\alpha$, $\overline{\alpha}$ and $-\overline{\alpha}$ also have this property. They are all units, not in the sense of Euclid but in a new sense: each of them divides all other numbers. If ρ' is the inverse of the unit ρ, then

$$\xi = \rho\rho'\xi = \rho\eta, \qquad \eta = \rho'\xi,$$

so that ρ divides all ξ in the domain.

Observe in general that if $\xi = a + b\alpha$, then

$$\mathrm{N}\,\xi = \xi\overline{\xi} = (a + b\alpha)(a + b\overline{\alpha}) = a^2 - ab + b^2 = \left(a - \frac{b}{2}\right)^2 + \frac{3b^2}{4}$$

is a positive integer and

$$\mathrm{N}(\xi\eta) = \xi\eta\overline{\xi\eta} = \xi\eta\overline{\xi}\,\overline{\eta} = (\mathrm{N}\,\xi)(\mathrm{N}\,\eta).$$

In particular if ξ is a unit, so that its inverse η is also in the domain, then $1 = \xi\eta$ and

$$1 = \mathrm{N}\,\xi\,\mathrm{N}\,\eta,$$

Units

$$1 \text{ and } -1.$$

$$\alpha = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \quad \text{and} \quad -\alpha = \frac{1}{2} - i\frac{\sqrt{3}}{2}.$$
$$\alpha^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2} \quad \text{and} \quad -\alpha^2 = \frac{1}{2} + i\frac{\sqrt{3}}{2}.$$

Units times λ

$$1 - \alpha, \quad -1 + \alpha.$$
$$\alpha - \alpha^2 = 1 + 2\alpha, \quad -1 - 2\alpha.$$
$$\alpha^2 - 1 = -2 - \alpha, \quad 2 + \alpha.$$

so that the positive integers $\mathrm{N}\,\xi$ and $\mathrm{N}\,\eta$ are both 1. Thus if $\xi = a + b\alpha$, then

$$4 = (2a - b)^2 + 3b^2.$$

For this b must be 0 or ± 1. If b is 0 then $a = \pm 1$ and $\xi = \pm 1$. If $b = \pm 1$, then $2a - b = \pm 1$ and $a = (\pm 1 \pm 1)/2$, which is 0 or b. Then

$$b + b\alpha = -b\alpha^2.$$

We conclude that the only units are those found, ± 1, $\pm\alpha$, $\pm\alpha^2$.

A number ξ in the domain $\mathbf{Z}(\alpha)$ will be called prime if in any representation

$$\xi = \eta\zeta,$$

one of η and ζ is necessarily a unit. If for example η is a unit, then

$$\zeta = \overline{\eta}\xi.$$

Some examples of primes

Observe that if $\mathrm{N}\,\xi$ is a prime then ξ is a prime, because if

$$\xi = \eta\zeta,$$

then

$$\mathrm{N}\,\xi = \mathrm{N}\,\eta\,\mathrm{N}\,\zeta,$$

so that either $\mathrm{N}\,\eta = 1$ or $\mathrm{N}\,\zeta = 1$ because $\mathrm{N}\,\xi$ cannot be factored. Consider for example $\lambda = 1 - \alpha$.

$$\mathrm{N}\,\lambda = (1 - \alpha)(1 - \overline{\alpha}) = (1 - \alpha)(1 - \alpha^2) = 1 - \alpha - \alpha^2 + 1 = 3,$$

so that λ is a prime and, indeed, a prime that divides 3. Moreover

$$\overline{\lambda} = 1 - \alpha^2 = -\alpha^2(1 - \alpha) = -\alpha^2\lambda = \rho\lambda,$$

where ρ is a unit. Thus

$$3 = \rho\lambda^2$$

is the factorization of 3, so that 3 is now, in essence, a square.

Examples of primes continued

In general, if n is a norm, then

$$4n = (2a - b)^2 + 3b^2.$$

I make a table of n for $a = -7, \ldots, 7$, $b = 0, \ldots, 7$. Since changing a to $-a$ and, at the same time, b to $-b$ does not change the norm, this table implicitly includes b from -7 to 7.

Some norms

$a\backslash b$	0	1	2	3	4	5	6	7
−7	49	57	67	79	93	109	127	147
−6	36	43	52	63	76	91	108	127
−5	25	31	39	49	36	75	91	109
−4	16	41	28	37	48	61	76	93
−3	9	13	19	27	37	49	63	79
−2	4	7	12	19	28	39	52	87
−1	1	3	7	13	21	31	43	57
0	0	1	4	9	16	25	36	49
1	1	1	3	7	13	21	31	43
2	4	3	4	7	12	19	28	39
3	9	7	7	12	13	19	27	37
4	16	13	12	13	16	21	28	37
5	25	21	19	19	21	25	31	39
6	36	31	28	27	28	31	36	43
7	49	43	39	37	37	39	43	49

Primes continued

Apart from 3, the primes that appear in this table are 7, 13, 19, 31, 43, 61, 67, 79. In principle, numbers that have the same norm appear in groups of six, each being obtained from the other by multiplying by a unit, or, if we demand that b be positive or zero and that a be positive when $b = 0$, in groups of three. The number 0 is an exception. For example, the following numbers have norm 3:

$$1 - \alpha, \quad -1 + \alpha, \quad \alpha - \alpha^2 = 2\alpha + 1,$$
$$-2\alpha - 1, \quad \alpha^2 - 1 = -2 - \alpha, \quad 2 + \alpha,$$

corresponding to $(-1, 1)$, $(1, 2)$, $(2, 1)$ and their negatives.

The number 7 appears in the table six times, thus there must be at least one pair ξ and η such that η is not a unit times ξ. The first number with norm 7 is $= -2 + \alpha$. We have then

$$-2 + \alpha, \quad -\alpha(-2 + \alpha) = 2\alpha - \alpha^2 = 1 + 3\alpha, \quad \alpha^2(-2 + \alpha) = 1 - 2\alpha^2 = 3 + 2\alpha,$$

accounting for three of the appearances of 7. The others are

$$-1 + 2\alpha, \quad -\alpha(-1 + 2\alpha) = \alpha - 2\alpha^2 = 2 + 3\alpha, \quad \alpha^2(-1 + 2\alpha) = 2 - \alpha^2 = 3 + \alpha.$$

Observe that any number of the first set is relatively prime to any number of the second set.

When verifying this, we had best use the modern notion of relatively prime, because we have not yet established any kind of euclidean algorithm for the domain $\mathbf{Z}(\alpha)$. Thus to say that two numbers ξ and ζ in the domain are relatively prime means that the collection of numbers $\mu\xi + \nu\zeta$, where μ and ν are arbitrary numbers in $\mathbf{Z}(\alpha)$ contains 1. Notice that this collection does not change if we replace ξ by $\epsilon\xi$, with ϵ a unit. We have then simply to replace μ by $\mu\epsilon'$, $\epsilon' = \bar{\epsilon} = 1/\epsilon$. Take then

$\xi = -2 + \alpha$ and $\zeta = 3 + \alpha$. Then $-\xi + \zeta = 5$ and $\xi\overline{\xi} = 7$. Since $3 \times 7 - 4 \times 5 = 1$, we have

$$(3\overline{\xi} + 4)\xi - 4\zeta = 1.$$

Primes continued

Primes that do not appear in the table are 2, 5, 11, 17, 23, 29. Each of these numbers is already a prime, although their norms are squares, $\mathrm{N}\,2 = 4$, $\mathrm{N}\,5 = 25$ and so on. If, for example, 2 were not a prime, we would have

$$2 = \xi\zeta, \quad 4 = \mathrm{N}\,2 = \mathrm{N}\,\xi\,\mathrm{N}\,\zeta,$$

with neither ξ nor ζ being a unit. Thus

$$2 = \mathrm{N}\,\xi = \mathrm{N}\,\zeta.$$

Suppose $\xi = a + b\alpha$. Then

$$2 = \mathrm{N}\,\xi = a^2 - ab + b^2$$

I calculate the remainder of each side on division by 3. On the left it is 2. On the right it depends only on the remainder left by a and b.

$$(a + 3c)^2 - (a + 3c)(b + 3d) + (b + 3d)^2 = a^2 - ab + b^2 + 3e$$

with

$$e = 2ac + 3c^2 - cb - ad - 3cd + 2bd + 3d^2.$$

So there are nine possibilities.

$a\backslash b$	0	1	2
0	0	1	1
1	1	1	0
2	0	1	1

So there is no question of the two sides having the same remainder and thus no question of the sides being equal. Since 5, 11, 17, 23 and 29 all leave the remainder 2 on division by 3, the same argument applies and they too cannot be factorized.

Some factorizations

$$\xi = -2 + \alpha = -\frac{5}{2} + \frac{\sqrt{3}}{3},$$

$$\overline{\xi} = -2 - 1 - \alpha = -3 - \alpha = -\frac{5}{2} + \frac{\sqrt{3}}{2}$$

$$\xi\overline{\xi} = \frac{25}{4} + \frac{3}{4} = 7.$$

Thus the prime 7 factors as $\xi\overline{xi}$ and ξ and $\overline{\xi}$ are relatively prime.

$$\xi = -2 + 3\alpha, \quad \overline{\xi} = -5 - 3\alpha, \quad \xi\overline{\xi} = N\xi = 19.$$

Thus the prime 19 factors as $\xi\overline{\xi}$ and ξ and $\overline{\xi}$ are relatively prime. If not *and if there were unique factorization* we would have $\xi = \mu\eta$, $\overline{\xi} = \nu\eta$, where η was not a unit, and

$$19^2 = \mathrm{N}\,\xi\,\mathrm{N}\,\overline{\xi} = \mathrm{N}\,\mu\,\mathrm{N}\,\nu\,\mathrm{N}\,\eta^2,$$

so that $\mathrm{N}\,\eta = 19$ and $\overline{\xi} = \rho\xi$ is a unit times ξ.

In general, if $\xi = a + b\alpha$ so that $\overline{\xi} = a - b - b\alpha$, then

$$\overline{\xi} = \xi \implies b = 0,$$

$$\overline{\xi} = -\xi \implies a = b - a \implies \xi = a(1 + 2\alpha),$$

so that $\xi = a\alpha\lambda$ is a multiple of λ,

$$\overline{\xi} = \alpha\xi \implies a - b - b\alpha = -b + (a - b)\alpha$$

or $a = 0$, $\xi = b\alpha$,

$$\overline{\xi} = -\alpha\xi \implies a - b - b\alpha = b + (b - a)\alpha,$$

so that $a = 2b$ and $\xi = -a\alpha^2\lambda$ is a multiple of λ,

$$\overline{\xi} = \alpha^2\xi \implies a - b - b\alpha = b - a - a\alpha$$

or $b = a$, so that $\xi = -a\alpha^2$,

$$\overline{\xi} = -\alpha^2\xi \implies a - b - b\alpha = a - b + a\alpha,$$

and $a = -b$ and $\xi = a\lambda$ is again a multiple of λ.

Thus, in general, *provided there is a unique factorization* we can expect that an ordinary prime that leaves the remainder 1 upon division by 3 is the product of two relatively prime numbers in $\mathbf{Z}(\alpha)$.

Just as the primes that do not appear all leave the remainder 2 upon division by 3, or as one says, they are all congruent to 2 modulo 3, so do all the primes, with the exception of 3 itself, that appear leave the remainder 1. The first primes of this sort that do not appear are 73 and 97. We can guess that this is because the table is too small. Indeed further calculations show that

$$\mathrm{N}(1 + 9\alpha) = 73, \qquad \mathrm{N}(3 + 11\alpha) = 97.$$

I shall present a proof of Fermat's theorem for $n = 3$ that depends on the possibility of factoring every element ξ of $\mathbf{Z}(\alpha)$ into primes, thus into a product

$$\xi = \epsilon\pi_1^{a_1}\pi_2^{a_2}\cdots$$

in which the factors are unique up to order and up to multiplication with a unit. The number ϵ is a unit.

Although we have some experience with ordinary primes and readily recognize the smaller of them, 2, 3, 5, 7 and so on, and can also find with no difficulty the prime factorization of small numbers,

$$98 = 2 \times 7^2,$$

this is by no means the case for larger numbers. The 1,000th prime is 7,919, but it is clear to none of us without either a good deal of calculation or a knowledge of special techniques how to verify that it is prime. The situation is even worse for numbers in $\mathbf{Z}(\alpha)$, and even excellent mathematicians can be led into error when they venture into this area without previous experience. Since I, too, in these lectures am dealing with material with which I have limited experience, I give, as a cautionary tale, an example from a book of a friend, a distinguished mathematician for whom I have great respect.

It is a book about the origins of modern algebra and, in particular, about the solution of equations, so that its aims are, in part, those of these lectures.

Some identities

Since $\alpha = (-1+\sqrt{-3})/2$, the numbers in $\mathbf{Z}(\alpha)$ are the numbers $(a+b\sqrt{-3})/2$, where a and b are both even. The book had been given to me by my friend in California. I was reading it with pleasure on the return flight when I came across the following passage.

In other words, we have the remarkable identity

$$2 = \sqrt[3]{6\sqrt{3}+10} - \sqrt[3]{6\sqrt{3}-10}.$$

Try proving this directly!!

I had seen such identities before and had indeed found them curious, but had never stopped to reflect on them. On the airplane, however, with these lectures in mind, I stopped to reflect on the identity and quickly came to the conclusion that the ideas introduced by Kummer and Galois, to whom we shall come, strongly suggest that any such identity has to be trivial. To be more precise, they suggest that such an identity only arises when the two numbers involved, $\xi = 6\sqrt{3}+10$ and $\zeta = 6\sqrt{3}-10$ are both cubes,

$$\xi = \mu^3, \qquad \zeta = -\nu^3,$$

and

$$\mu + \nu = 2.$$

To test this, we first calculate an analogue of the norm of ξ, multiplying ξ by $\xi' = -6\sqrt{3}+10$,

$$\xi\xi' = (6\sqrt{3}+10)(-6\sqrt{3}+10) = -108+100 = -8,$$

which is indeed a cube, $-8 = (-2)^3$. Thus if we could find a number, whose norm (in this new sense) is -2, we would have a start on finding μ.

The norm of $a+b\sqrt{3}$ is

$$(a+b\sqrt{3})(a-b\sqrt{3}) = a^2 - 3b^2,$$

so that $a = \pm 1$, $b = \pm 1$ are four possibilities for a number whose norm is -2. Since

$$(1+\sqrt{3})^2 = 1+2\sqrt{3}+3 = 4+2\sqrt{3},$$

and

$$(1+\sqrt{3})(4+2\sqrt{3}) = 4+4\sqrt{3}+2\sqrt{3}+6 = 10+6\sqrt{3},$$

one possibility for μ is $1+\sqrt{3}$. In the same way, we can take $\nu = 1-\sqrt{3}$. Since

$$\mu + \nu = 2,$$

the identity is not remarkable. It just appears on first sight to be so.

Unfortunately with a tactlessness that I exhibit only too frequently, I sent off an e-mail message to my friend upon my return, expressing the hope that his students had not allowed him to pull the wool over their eyes. It was not the right response to his enthusiasm or his generosity. I hope he has forgiven me.

As an exercise, whose solution will be given next week, I let you show that for similar reasons the identity

$$1 = \sqrt[3]{2\sqrt{13}+5} - \sqrt[3]{2\sqrt{13}-5},$$

which appears in the same book as an exercise, is also not remarkable!

Since the book is, in spite of my teasing, an excellent book that you might well enjoy, I give the author and title:

V. S. Varadarajan, *Algebra in ancient and modern times*.

Solution to exercise

The first step is to calculate the norm of $2\sqrt{13}+5$. It is

$$(2\sqrt{13}+5)(-2\sqrt{13}+5) = -52+25 = -27,$$

so that our first step is to find a number μ whose norm is -3. This is easy, for

$$(7+2\sqrt{13})(7-2\sqrt{13}) = 49-52 = -3.$$

Since

$$(7+2\sqrt{13})+(7-2\sqrt{13}) = 14,$$

this will not serve our purpose. Indeed we need a number of the form

$$\frac{1}{2}+b\sqrt{13},$$

so that

$$\left(\frac{1}{2}+b\sqrt{13}\right)+\left(\frac{1}{2}-b\sqrt{13}\right) = 1.$$

We need in addition,

$$\left(\frac{1}{2}+b\sqrt{13}\right)\left(\frac{1}{2}-b\sqrt{13}\right) = \frac{1}{4}-13b^2 = -3,$$

or

$$-13b^2 = -\frac{13}{4}.$$

Thus $b = 1/2$, $\mu = (1+\sqrt{13})/2$ and $\nu = (1-\sqrt{13})/2$.

Since

$$\left(\frac{1}{2}+\frac{1}{2}\sqrt{13}\right)^2 = \frac{7}{2}+\frac{1}{2}\sqrt{13},$$

we have

$$\left(\frac{1}{2}+\frac{1}{2}\sqrt{13}\right)^3 = \left(\frac{1}{2}+\frac{1}{2}\sqrt{13}\right)\left(\frac{7}{2}+\frac{1}{2}\sqrt{13}\right) = 5+2\sqrt{13}.$$

Since $5+2\sqrt{13}$ looks to be an integer, it is natural to suppose that its cube root, $\mu = (1+\sqrt{13})/2$ is also an integer. This raises the question as to when a number of some complicated form is to be regarded as integral. Although the answer is simple, it is not so easy to justify it. So I pass over the matter quickly remarking only that the numbers we shall meet will by and large be integral. I observe in addition that μ and ν satisfy the equation

$$0 = (x-\mu)(x-\nu) = x^2-x+3,$$

in which the coefficient of x^2 is 1 and all other coefficients ordinary integers.

Lecture 3 [Lecture 11]

Mathematical transition

For the construction of the regular pentagon, we used the five solutions, z_0, z_1, z_2, z_3, z_4, of

$$Z^5 - 1 = 0,$$

thus the five numbers

$$z_k = \cos(2\pi k/5) + i\sin(2\pi k/5), \qquad k = 0, 1, 2, 3, 4.$$

The first of these is just 1 and was of little interest. All the others were from an *algebraic* point of view equivalent and all satisfied the equation

$$Z^4 + Z^3 + Z^2 + Z + 1 = 0.$$

We could have singled out $\cos(2\pi/5) + i\sin(2\pi/5)$ as being from a *geometrical* point of view the obvious choice.

For the construction of the regular heptadecagon, we used the sixteen solutions, z_1, z_2, z_3, z_4, z_5, z_6, z_7, z_8, z_9, z_{10}, z_{11}, z_{12}, z_{13}, z_{14}, z_{15}, z_{16}, of

$$Z^{16} + Z^{15} + Z^{14} + \cdots + Z^1 + 1 = 0.$$

They are

$$z_k = \cos(2\pi k/17) + i\sin(2\pi k/17).$$

In both cases, it was the symmetries that were of principal interest and what we studied was the effect of these symmetries not alone on $z_1, z_2, \ldots$ but on all the numbers

$$a_1 z_1 + a_2 z_2 + a_3 z_3 + \cdots,$$

where $a_1, a_2, a_3, \ldots$ were arbitrary rational numbers, thus fractions.

If we had studied the equilateral triangle, which we left aside as too simple, we would have used the three numbers

$$z_k = \cos(2\pi k/3) + i\sin(3\pi k/3), \qquad k = 0, 1, 2,$$

of which now only two are of much algebraic interest, namely

$$z_1 = \cos(2\pi/3) + i\sin(2\pi/3), \quad z_2 = \cos(2\pi/3) - i\sin(2\pi/3).$$

Both satisfy the equation

$$Z^2 + Z + 1 = 0,$$

which can be solved to yield

$$\frac{-1 \pm \sqrt{1-4}}{2} = \frac{-1 \pm \sqrt{-3}}{2} = \frac{-1 \pm i\sqrt{3}}{2}$$

Date of lecture: Spring term, February 15, 2000.

Comparing signs, we see that

$$z_1 = \frac{-1 + i\sqrt{3}}{2}$$

This is the number that I now call simply α. This is partly because, as often happens, I have simply taken over a notation from others, but also because we are interested in quite different properties of the numbers

$$a_1 z_1 + a_2 z_2$$

or, more generally, if we were studying Fermat's equation for $n = 5$, $n = 17$ or any other prime of the numbers

$$a_1 z_1 + a_2 z_2 + \cdots + a_{n-2} z_{n-2} + a_{n-1} z_{n-1},$$

where, for example, $n - 1$ is 4 if $n = 5$ or 16 if $n = 17$.

For the moment, since these properties are rather difficult, we confine ourselves to $n = 3$. Then

$$a_1 z_1 + a_2 z_2 = a_1 \alpha + a_2 \alpha^2 = a_1 \alpha - a_2(1 + \alpha) = a + b\alpha,$$

with $a = -a_2$, $b = a_1 - a_2$.

In the earlier approaches to Fermat's theorem, for $n = 3$ in particular, what is important are primes: ordinary primes in Euler's treatment and primes in a more exotic setting for a treatment modelled on Kummer's general methods. Primes are integers. So we need to use only integral numbers of the form $a + b\alpha$. We can naively expect that such a number will be integral if a and b are not merely rational numbers but in fact whole numbers, that is integers. The naive expectation is borne out by experience. I even give the domain of such numbers a special symbol $\mathbf{Z}(\alpha)$. The domain for $n = 3$ is much simpler than it will be for $n > 3$.

Any complex number is represented in the plane. This is true not only of α but of all the numbers $a + b\alpha$. The norm of a complex number $z = x + iy$ is *for us* the *square* of its distance from the origin. Thus the norm of $1 + i$ is 2, that of $2 + 7i$ is $4 + 49 = 53$. This norm is

$$z\overline{z} = (x + yi) \times (x - yi) = x^2 + y^2.$$

Thus the norm of α is

$$\cos^2(2\pi/3) + \sin^2(2\pi/3) = \frac{1}{4} + \frac{3}{4} = 1,$$

and so is that of $\alpha^2 = -1 - \alpha = \overline{\alpha}$,

$$\alpha^2 = \frac{-1 - i\sqrt{3}}{2}.$$

More about norms

We have stressed that $z \to \overline{z}$ is a symmetry of the collection of complex numbers, which arises because i and $-i$ are both algebraic symbols with exactly the same properties. The distinction between the two only arises in the geometric representation. The point representing i lies above the axis of abscissas and the point representing $-i$ lies below it. Since it is a symmetry—as is readily verified—it must respect multiplication

$$\overline{w} \times \overline{z} = \overline{z \times w}.$$

Thus

$$\mathrm{N}(z \cdot w) = (z \cdot w) \cdot (\overline{z \cdot w}) = z \cdot w \cdot \overline{z} \cdot \overline{w} = z\overline{z} \cdot w\overline{w} = \mathrm{N}\, z \cdot \mathrm{N}\, w.$$

This formal property appears for other definitions of norms, norms that have no relation to length. Consider, for example, a new domain, the domain of numbers $c + d\sqrt{3}$, where c and d are now integers. It is different from $\mathbf{Z}(\alpha)$ because

$$a + b\alpha = \left(a - \frac{b}{2}\right) + \frac{b}{2}\sqrt{-3} = c + d\sqrt{-3}.$$

Not only is -3 replaced by 3, the important point, but in the new domain the coefficients c and d are to be whole numbers, whereas in $\mathbf{Z}(\alpha)$, they may be half-integers. The second point is too subtle for us to linger on it here. It arises because

$$\mathrm{N}\left(\frac{1}{2} + \frac{1}{2}\sqrt{-3}\right) = \frac{1}{4} + \frac{3}{4} = 1$$

is integral.

On the other hand in the new domain there is also a symmetry. It sends $\sqrt{3}$ to $-\sqrt{3}$ and thus

$$c + d\sqrt{3} \to c - d\sqrt{3}.$$

Since $\sqrt{3}$ and $-\sqrt{3}$ satisfy exactly the same equation with rational coefficients, namely

$$Z^2 - 3 = 0,$$

they are indistinguishable if one's only reference points are rational numbers. That is what permits the symmetry.

Thus

$$\begin{array}{c} (a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc) \\ \downarrow \\ (ac + 3bd) - (ad + bc)\sqrt{3} = (a - b\sqrt{3})(c - d\sqrt{3}) \end{array}$$

and

$$\begin{array}{c} (a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + (b + d\sqrt{3}) \\ \downarrow \\ (a + c) - (b + d)\sqrt{3} = (a - b\sqrt{3}) + (c - d\sqrt{3}) \end{array}$$

This new and different norm was the norm that we used to study the identity

$$2 = \sqrt[3]{6\sqrt{3} + 10} - \sqrt[3]{6\sqrt{3} - 10}. \tag{A}$$

We noted that

$$\mathrm{N}(6\sqrt{3} + 10) = 100 - 3 \cdot 36 = -8$$

and that -8 was a cube.

The numbers in the new domain are all real and the norm is no longer a distance. It is just a convenient algebraic device. If we want to think of $\sqrt{3}$ as an ordinary real number then it is approximately 1.73205. Thus $1 + \sqrt{3}$ is approximately 2.73205 and $1 - \sqrt{3}$ is approximately -0.73205 but their product, which is the norm of either is -2. Another example is $17 - 10\sqrt{3}$ which under the symmetry becomes $17 + 10\sqrt{3}$. Their norm is

$$(17 - 10\sqrt{3})(17 + 10\sqrt{3}) = 289 - 300 = -11.$$

These numbers are as decimals approximately -0.320508 and 34.3205, but in algebraic investigations their decimal expansion should be studiously ignored. It is irrelevant!

The identity (A) is valid. The question is whether it is remarkable. It certainly appears strange. My point was that it is striking not because it expresses any profound or even curious mathematical truth, but only because our unfamiliarity with numbers formed from surds prevents our recognizing easily that both the numbers under the cube-root signs are cubes. Once we do so, we see that the identity becomes

$$\sqrt[3]{(1+\sqrt{3})^3} + \sqrt[3]{(1-\sqrt{3})^3} = 2,$$

and no one would claim that this is remarkable. It is trivial!

Afterthought

The remarkable formula is a consequence of a general formula, the formula of Del Ferro, for the solution of a cubic equation.

$$X^3 + PX = Q$$

$$\Delta = \frac{Q^2}{4} + \frac{P^3}{27}$$

$$X = \sqrt[3]{\sqrt{\Delta} + \frac{Q}{2}} - \sqrt[3]{\sqrt{\Delta} - \frac{Q}{2}}$$

This is of course, as Varadarajan remarks, a very beautiful formula, even today. Applied to

$$X^3 + 6X = 20,$$

which has the root 2, it yields the initial identity

$$\text{(A)} \qquad \sqrt[3]{6\sqrt{3}+10} - \sqrt[3]{6\sqrt{3}-10}.$$

Del Ferro's dates are 1465–1526, thus long before Kummer and Galois. In the fifteenth or sixteenth century, recognizing that a number formed from the square root of 3 was a cube was an altogether different matter than it is today. So, if the formula was regarded as remarkable then, it was with good reason. Once again, I have to admit that I am unfamiliar with the response to such formulas at the time of their discovery and subsequently.

On the other hand, I began by observing that it is only familiarity with the ideas of Kummer and Galois that made me suspicious, and the reason for introducing the example is not to suggest that someone unfamiliar with what might be called higher mathematics or modern algebra has no right to be astonished, but rather to emphasize that calculations within domains such as $\mathbf{Z}(\alpha)$ or

$$\mathbf{Z}(\sqrt{3}) = \left\{ a + b\sqrt{3} \;\middle|\; a, b \in \mathbf{Z} \right\}$$

are not easily made and require practice and experience. We are trying to acquire them.

When we come to Kummer, we shall see that he replaces the solution $\alpha = \cos(2\pi/3) + i\sin(2\pi/3)$ of

$$Z^2 + Z + 1 = 0$$

by the solution $\alpha = \cos(2\pi/n) + i\sin(2\pi/n)$ of

$$Z^{n-1} + Z^{n-2} + Z^{n-3} + \cdots + Z^2 + Z + 1 = 0,$$

The number n becoming an arbitrary odd prime.

$$n = 3, 5, 7, 11, 13, 17, 19, 23, 31, \ldots,$$

23 being particularly fateful. The domain $\mathbf{Z}(\alpha)$ is different in each case.

There are two difficulties that appear, one immediately for $n = 5$. The first is that there are no longer just a finite number of units to cause trouble. For $n > 3$, there are an infinite number. The second is that from 23 on there is no longer unique factorization. Thus before we see how Kummer was able to overcome these problems, we had best understand in the simplest case, $n = 3$, what difficulties the units cause and what advantages unique factorization possesses, even indeed what unique factorization is. How can it be exploited to prove Fermat's theorem for $n = 3$? We will then be in a better position to appreciate Kummer's achievement in doing without it. Euclid's discussion of primes and of the greatest common measure of two numbers is perhaps of considerable historical interest, but, I now see, hardly the right introduction to an adequate understanding of the modern notion.

Some names and dates

Carl Friedrich Gauß (1777–1855)

Gabriel Lamé (1795–1870)

Niels Henrik Abel (1802–1829)

Carl Gustav Jacob Jacobi (1804–1851)

Peter Gustav Lejeune Dirichlet (1805–1859)

Ernst Eduard Kummer (1810–1893)

Leopold Kronecker (1823–1891)

Gotthold Eisenstein (1823–1852)

Richard Dedekind (1831–1916)

Disquisitiones Arithmeticae 1801

Some background reading

- Two articles by H. M. Edwards in the *Archive for the History of Exact Sciences*.
- *The Background of Kummer's Proof of Fermat's Last Theorem for Regular Primes*, vol. 14.
- Postscript to "*The Background of Kummer's Proof*", vol. 17.

Historical transition

There is also a historical transition on which it would be agreeable to spend some time, but only if I had sufficient familiarity with the mathematical literature and correspondence of the period. Since I do not, I shall be brief.

If $\alpha = \cos(2\pi/n) + i\sin(2\pi/n)$ the study of numbers

$$a + b\alpha + c\alpha^2 + \cdots,$$

with $a, b, c, \ldots$ rational or integral is known as cyclotomy. As the name suggests and as we learned from Gauss, these numbers are the algebraic instruments for examining the division of the circle into n equal parts.

They have other uses, one of which, at least in certain cases, was discovered by Gauss, and was popular among young mathematicians of the succeeding generations, especially, Jacobi, Kummer, Eisenstein. The achievement of the young Gauss that mathematicians are inclined to emphasize is not the construction of the regular heptadecagon but the first complete, adequate proof of the law of quadratic reciprocity.

Consider the following sequence of numbers.

$$x^2 + 1, \qquad x = 1, \ldots, 20$$

2, 5, 10, 17, 26, 37, 50, 65, 82, 101, 122,
145, 170, 197, 226, 257, 290, 325, 362, 401

Factored.

$2, 5, 2\cdot 5, 17, 2\cdot 13, 37, 2\cdot 5^2, 5\cdot 13, 2\cdot 41, 101, 2\cdot 61, 5\cdot 29, 2\cdot 5\cdot 17, 197,$
$2\cdot 113, 257, 2\cdot 5\cdot 29, 5^2\cdot 13, 2\cdot 181, 401.$

With the exception of 2, all the primes that appear in these factorizations leave the remainder 1 upon division by 4.

GEDÄCHTNISSREDE AUF GUSTAV PETER LEJEUNE DIRICHLET

VON

E. E. KUMMER.

[Gelesen in der öffentlichen Sitzung der Königl. Akademie der Wissenschaften am 5. Juli 1860.]

Es ist nicht zehn Jahre her, dass die drei Männer, denen unser deutsches Vaterland eine neue Blüthenperiode der mathematischen Wissenschaften verdankt, GAUSS, JACOBI und DIRICHLET noch lebten und noch thätig arbeiteten, den alten Ruhm tiefer Erkenntniss der abstractesten, sowie der concret in der Natur verwirklichten mathematischen Wahrheiten, welchen vor allen KEPLER und LEIBNITZ der deutschen Nation erworben hatten, glänzend zu erneuern und zu befestigen. Unsere Akademie hatte damals das Glück, zwei dieser hervorragenden Männer als active Mitglieder zu besitzen, JACOBI und DIRICHLET, welche persönlich befreundet, durch freie Mittheilung ihrer tiefen mathematischen Gedanken sich gegenseitig anregten und förderten, und auf die allgemeine Entwickelung der mathematischen Wissenschaften den nachhaltigsten Einfluss ausübten. JACOBI's frühzeitiger Tod war der erste unersetzliche Verlust, welcher die in unserem Vaterlande zur Blüthe entfaltete Wissenschaft traf. Die Bedeutung der Schöpfungen dieses mit seltenem Geiste begabten Forschers, die hervorragende Stellung, die er in der Geschichte der Mathematik für alle Zeiten einnehmen wird, hat DIRICHLET in der heut vor acht Jahren an dieser Stelle gehaltenen Gedächtnissrede so tiefeingehend und wahr geschildert, dass er dadurch dem Andenken des Dahingeschiedenen das schönste und würdigste Denkmal errichtet hat. Als vier Jahre nach JACOBI der greise GAUSS in dem unbestrittenen Ruhme des ersten Mathematikers seiner Zeit aus dem Leben schied, hatte dieser grosse allgemeine Verlust für unsere Akademie noch die beklagenswerthe Folge, dass DIRICHLET, als der einzige würdige Nachfolger des grossen Mannes, nach

Consider another sequence.

$$x^2 + 3, \qquad x = 1, \ldots, 20$$

4, 7, 12, 19, 28, 39, 52, 67, 84, 103, 124,
147, 172, 199, 228, 259, 292, 327, 364, 403

Factored.

2^2, 7, $2^2 \cdot 3$, 19, $2^2 \cdot 7$, $3 \cdot 13$, $2^2 \cdot 13$, 67, $2^2 \cdot 3 \cdot 7$, 103, $2^2 \cdot 31$, $3 \cdot 7^2$, $2^2 \cdot 43$, 199,
$2^2 \cdot 3 \cdot 19$, $7 \cdot 37$, $2^2 \cdot 73$, $3 \cdot 109$, $2^2 \cdot 7 \cdot 13$, $13 \cdot 31$.

With the exception of 2 and 3 all the primes that appear as factors leave the remainder 1 upon division by 3.

Consider now the somewhat more mysterious sequence.

$$x^2 - 3, \qquad x = 1, \ldots, 20$$

−2, 1, 6, 13, 22, 33, 46, 61, 78, 97, 118, 141,
166, 193, 222, 253, 286, 321, 358, 397

Factored.

$-1 \cdot 2$, 1, $2 \cdot 3$, 13, $2 \cdot 11$, $3 \cdot 11$, $2 \cdot 23$, 61, $2 \cdot 3 \cdot 13$, 97, $2 \cdot 59$, $3 \cdot 47$, $2 \cdot 83$,
193, $2 \cdot 3 \cdot 37$, $11 \cdot 23$, $2 \cdot 11 \cdot 13$, $3 \cdot 107$, $2 \cdot 179$, 397

The primes here, those different from 2 and 3, leave both the remainders 1 and 3 upon division by 4 and the remainders 1 and 2 upon division by 3. So a rule is not at first apparent. One is quickly found. For example, 13 leaves the remainder 1 upon division by 4 and upon division by 3. On the other hand, 11 leaves the remainder 3 upon division by 4 and the remainder 2 upon division by 3. The same is true of 23, whereas 61 behaves like 13, as does 97. On examination of the other primes in the factorization, this appears to be a general rule.

These general rules appear for other expressions of the form $x^2 \pm p$, where p is a prime. They are called, for reasons that are not apparent and not so important, reciprocity laws. As one more example, consider $p = 5$.

$$x^2 - 5, \qquad x = 1, \ldots, 20$$

−4, −1, 4, 11, 20, 31, 44, 59, 76, 95, 116, 139,
164, 191, 220, 251, 284, 319, 356, 395

Factored.

-2^2, -1, 2^2, 11, $2^2 \cdot 5$, 31, $2^2 \cdot 11$, 59, $2^2 \cdot 19$, $5 \cdot 19$, $2^2 \cdot 29$, 139, $2^2 \cdot 41$,
191, $2^2 \cdot 5 \cdot 11$, 251, $2^2 \cdot 71$, $11 \cdot 29$, $2^2 \cdot 89$, $5 \cdot 79$.

The primes that appear here, with the exception of 2 and 5, all leave the remainder 1 or the remainder 4 upon division by 5. They do not leave the remainder 2 or 3.

The quadratic reciprocity law was formulated in general during the latter part of the eighteenth century, above all by Adrien-Marie Legendre, and was proved at the very end of the century by the young Gauss.

There are also higher reciprocity laws, for $x^m \pm p$, $m = 3, 4, 5, \ldots$, but they cannot be expressed without cyclotomy. Even the quadratic reciprocity law is intimately related to cyclotomy as we shall have occasion to see. I confess that, as a student unaware of the history of the subject and unaware of the connection with cyclotomy, I did not find the law or its so-called elementary proofs appealing. I suppose, although I would not have—and could not have—expressed myself in this way that I saw it as little more than a mathematical curiosity, fit more for amateurs than for the attention of the serious mathematician that I then hoped to become. It was only in Hermann Weyl's book on the algebraic theory of numbers that I appreciated it as anything more. It is perhaps time for me to reread Weyl's book, a strange lumbering book, informed by an intellectual tension—conflict would be an inappropriate word—between two approaches to the theory, two approaches symbolized for Weyl by Kronecker and Dedekind, a tension that is still with us and, perhaps, still unresolved. Where, in the theory of numbers, do numbers end and geometry begin? The tension is, fortunately, not germane to Kummer although it does appear again, but not very obviously, in the aftermath of the recent proof of Fermat's theorem. There are some mathematicians who now place, in my view, too high hopes on the geometry. But these are arcane questions of interest to very few and their resolution will depend on results!

Although both Lagrange and Gauss were aware of possible applications of cyclotomy to Fermat's theorem, it was at first applied more to reciprocity laws. I add that reciprocity laws were every bit as important to Kummer as Fermat's theorem and were what first led him to take up cyclotomy. Reciprocity laws led to developments quite independent of Fermat that remain important to this day and that, indeed, were not of negligible import for the final resolution of the theorem.

Certainly the study of reciprocity laws entailed the study of factorization in the domains $\mathbf{Z}(\alpha)$, so that Jacobi, for example, had had some experience with it and was able to prevent Kummer from publishing at the very beginning of his study of cyclotomy some false conclusions.

"Der gute Junge" as he calls him in a letter to Dirichlet, with a certain condescension as he was only six years older, had without much ado assumed the decomposition of a prime $p = \lambda n + 1$ in complexes of numbers formed from the λth roots of unity and deduced general theorems from this.

Si l'on faisait $x = 0$ et $\xi = 0$, les quantités P et Π deviendraient

$$t^3 + Au^3 \quad \text{et} \quad \theta^3 + Av^3,$$

mais leur produit ne serait plus de la même forme, à cause que la quantité X ne deviendrait pas nulle.

Soit $n = 4$, en sorte que

$$p = t - ua\sqrt[4]{A} + xa^2\sqrt[4]{A^2} + ya^3\sqrt[4]{A^3} \quad \text{et} \quad a^4 - 1 = 0,$$

on trouvera

$$P = t^4 - A[2t^2(x^2 - uy) - 4tu^2x + u^4] + A^2(4txy^2 + x^4 - 4ux^2y + 2u^2y^2) - A^3y^4,$$

et le produit d'autant de fonctions de cette forme qu'on voudra sera toujours une fonction de la même forme, et ainsi de suite.

IV.

Si l'on avait à résoudre l'équation

$$r^n - As^n = q^m,$$

il est évident qu'on y parviendrait si l'on pouvait rendre chaque facteur de $r^n - As^n$, comme $r - as\sqrt[n]{A}$, égal à une puissance $m^{ième}$, a étant toujours une des racines de l'équation $a^n - 1 = 0$.

Soit donc en général

$$r - sa\sqrt[n]{A} = p^m,$$

en sorte que

$$p = \sqrt[m]{r - sa\sqrt[n]{A}},$$

il est facile de concevoir que la valeur de p ne peut être exprimée que de cette manière

$$p = t - ua\sqrt[n]{A} + xa^2\sqrt[n]{A^2} + ya^3\sqrt[n]{A^3} + \ldots + za^{n-1}\sqrt[n]{A^{n-1}};$$

cette quantité étant élevée à la puissance m, on aura (numéro précédent)

$$p^m = T + Va\sqrt[n]{A} + Xa^2\sqrt[n]{A^2} + Ya^3\sqrt[n]{A^3} + \ldots + Za^{n-1}\sqrt[n]{A^{n-1}};$$

Mais, comme nous ne nous proposons pas ici de traiter cette matière à fond, nous ne nous y arrêterons pas davantage quant à présent: nous observerons seulement que M. de Fermat prétend, dans ses *Remarques sur Diophante*, avoir démontré en général ce théorème, que l'équation

$$r^n + s^n = q^n$$

n'est jamais résoluble d'une manière rationnelle lorsque n surpasse 2; mais ce Savant ne nous a pas laissé sa démonstration, et il ne paraît pas que personne l'ait encore trouvée jusqu'à présent. M. Euler a, à la vérité, démontré ce théorème dans le cas de $n = 3$ et de $n = 4$, par une analyse particulière et très-ingénieuse, mais qui ne paraît pas applicable en général à tous les autres cas; ainsi, ce théorème est un de ceux qui restent encore à démontrer, et qui méritent le plus l'attention des Géomètres.

était restée propre aux entiers rationnels jusqu'au milieu du XVIII^e siècle. C'est Euler qui, en 1770, ouvre un nouveau chapitre de l'Arithmétique en étendant, non sans témérité, la notion de divisibilité aux entiers d'une extension quadratique : cherchant à déterminer les diviseurs d'un nombre de la forme $x^2 + cy^2$ (x, y, c entiers rationnels), il pose $x + y\sqrt{-c} = (p + q\sqrt{-c})(r + s\sqrt{-c})$ (p, q, r, s entiers rationnels) et en prenant les normes des deux membres, il n'hésite pas à affirmer qu'il obtient ainsi tous les diviseurs de $x^2 + cy^2$ sous la forme $p^2 + cq^2$ ([*81* a], (1), t. I, p. 422). En d'autres termes, Euler raisonne comme si l'anneau $\mathbf{Z}[\sqrt{-c}]$ était principal ; un peu plus loin, il utilise un raisonnement analogue pour appliquer la méthode de « descente infinie » à l'équation $x^3 + y^3 = z^3$ (il se ramène à écrire que $p^2 + 3q^2$ est un cube, ce qu'il fait en posant $p + q\sqrt{-3} = (r + s\sqrt{-3})^3$). Mais dès 1773, Lagrange démontre ([*140*], t. III, p. 695-795) que les diviseurs des nombres de la forme $x^2 + cy^2$ ne sont pas toujours de cette forme, premier exemple de la difficulté fondamentale qui allait se présenter avec bien plus de netteté dans les études, poursuivies par Gauss et ses successeurs, sur la divisibilité dans les corps de racines de l'unité * ; il n'est pas possible, en général, d'étendre directement à ces corps les propriétés essentielles de la divisibilité des entiers rationnels, existence du p.g.c.d. et unicité de la décomposition en facteurs premiers. Ce n'est pas ici le lieu de décrire en détail comment Kummer pour les corps de racines de l'unité [*138*] **, puis Dedekind et Kronecker pour les corps de nombres algébriques quelconques, parvinrent à surmonter ce formidable obstacle par la création de la théorie des idéaux, un des progrès les plus décisifs de l'algèbre moderne. Mais Dedekind,

* Gauss semble avoir un moment espéré que l'anneau des entiers dans le corps des racines n-èmes de l'unité soit un anneau principal ; dans un manuscrit non publié de son vivant ([*95* a], t. II, p. 387-397), on le voit démontrer l'existence d'un processus de division euclidienne dans le corps des racines cubiques de l'unité, et donner quelques indications sur un processus analogue dans le corps des racines 5-èmes ; il utilise ces résultats pour démontrer par un raisonnement de « descente infinie » plus correct que celui d'Euler l'impossibilité de l'équation $x^3 - y^3 = z^3$ dans le corps des racines cubiques de l'unité, signale qu'on peut étendre la méthode à l'équation $x^5 + y^5 = z^5$, mais s'arrête à l'équation $x^7 + y^7 = z^7$ en constatant qu'il est impossible alors de rejeter *a priori* le cas où x, y, z ne sont pas divisibles par 7.

** Dès son premier travail sur les « nombres idéaux », Kummer signale explicitement la possibilité d'appliquer sa méthode, non seulement aux corps de racines de l'unité, mais aussi aux corps quadratiques, et de retrouver ainsi les résultats de Gauss sur les formes quadratiques binaires ([*138*], p. 324-325).

Lecture 4 [Lecture 12]

Leonhard Euler (1707–1783)

Date of lecture: Spring term, February 22, 2000.

Euler's algebra

The impossibility of finding a solution in integers of the equation

$$x^4 + y^4 = z^4$$

or even of the equation

$$x^4 + y^4 = z^2$$

was established by Fermat. It appears to have been Euler who in his textbook *Algebra*, published in 1770, first established the impossibility of solving the equation

$$x^3 + y^3 = z^3.$$

It is reported in a standard history that he obtained his proof sometime between 1753 and the time of publication. There is a gap in his proof that was filled by Legendre and to which we shall return. In essence, it can only be filled by understanding the decomposition into primes of numbers in $\mathbf{Z}(\alpha)$.

I observe in passing that Euler's algebra was a widely used textbook for some time. There is still much to recommend it today to the intelligent amateur. I like to imagine Clausewitz, who began the study of mathematics as a diversion after being taken prisoner by Napoleon's troops during the battle of Jena, working through a copy of *Algebra*. He writes to his fiancée of his studies, but unfortunately does not indicate what books he is using.

Euler's book starts at the beginning, and even has problems in what is presently a very hot topic, financial mathematics. I give two examples.

§II.1.36) *Ich habe einige Ellen Tuch gekauft und für jede 5 Ellen 7 Rthlr. bezahlt, davon wieder 7 Ellen für 11 Rhtlr. verkauft und dabei 100 Rthlr. gewonnen. Wie viel Tuch ist es gewesen?*

§II.1.26) *Ein Mann hinterläßt 11000 Rthlr. für seine Witwe, zwei Söhne und drei Töchter. Nach seinem Testamente soll die Frau zweimal mehr bekommen als ein Sohn, und ein Sohn zweimal mehr als eine Tochter. Wie viel bekommt jeder Erbe?*

Corrections and elaborations

There are a number of statements on the previous page that I have taken from various sources and that are doubtful, as is made clear by an examination of Weil's book on the history of the theory of numbers. First of all, Weil explains why there is good reason to believe that Fermat had not merely stated but in fact proved the impossibility of the equation

$$x^3 + y^3 = z^3, \qquad xyz \neq 0,$$

in integers. The proof, however, is not extant, the first extant proof being due to Euler. Moreover, although Euler is a little careless in his *Algebra* about the matter, the "gap" in his proof is filled by theorems that he had already proved and published in 1759. A complete proof does appear in Legendre's *Théorie des nombres* published in 1798. This may be the source of the error.

I shall give two apparently different proofs of the impossibility of this equation. In essence they are the same. One is that of Euler (and perhaps also that of Fermat). The other is modelled on later, more general, methods of Kummer and is meant as an aid to the understanding of his arguments.

These problems appear about half-way through the textbook. By the end, he has arrived at Fermat's theorem for cubes. In between (§II.2.188), he asks and partially answers when an expression $ax^2 + cy^2$ is a cube. He suggests setting

$$x\sqrt{a} + y\sqrt{-c} = (p\sqrt{a} + q\sqrt{-c})^3 \tag{A}$$

and

$$x\sqrt{a} - y\sqrt{-c} = (p\sqrt{a} - q\sqrt{-c})^3.$$

This makes

$$\begin{aligned} ax^2 + cy^2 &= (x\sqrt{a} + y\sqrt{-c})(x\sqrt{a} - y\sqrt{-c}) \\ &= \Big((p\sqrt{a} + q\sqrt{-c})(p\sqrt{a} - q\sqrt{-c})\Big)^3 \\ &= (ap^2 + cq^2)^3 \end{aligned} \tag{B}$$

If we expand the right side of (A), we obtain

$$(p^3a - 3pq^2c)\sqrt{a} + (3p^2aq - q^3c)\sqrt{-c},$$

so that (A) can be interpreted as the pair of equations,

$$x = p^3a - 3pq^2c, \qquad y = 3p^2aq - q^3c. \tag{C}$$

Thus these values for x and y ensure that $ax^2 + cy^2$ is a cube. Euler does not, however, show that, conversely, if $ax^2 + cy^2$ is a cube then integers p and q can be found that satisfy (C). None the less he uses this converse statement in his proof of Fermat's theorem for the prime 3. So his argument is incomplete. I present it nevertheless, completing it later.

It appears in the very last chapter of the very last section of the very last part of the book, in the section entitled, *von der unbestimmten Analytik*, which seems to be the late eighteenth, early nineteenth century term for the search for integral solutions to equations whose solutions are not uniquely determined. In the last chapter, the problem is to find two integers x and y such that the sum of their cubes is again a cube, thus to solve Fermat's equation

$$x^3 + y^3 = z^3.$$

Now Euler has already introduced in this section some techniques for solving such equations. I give examples that illustrate Euler's expository style and that illustrate as well some of the principal achievements of number theory before the appearance of Gauss. All of this material remained after Gauss and remains today a basic and integral part of the theory of numbers.

In §II.2.41 he asks when a rational number x can be found such that the rational number $x^2 + 1$ is a square. He observes that this is certainly possible. For example, is $x = 3/4$ then

$$x^2 + 1 = \frac{9}{16} + 1 = \frac{25}{16} = \left(\frac{5}{4}\right)^2.$$

This is of course familiar to us as

$$3^2 + 4^2 = 5^2,$$

because 3 and 4 are two sides of a right-angles triangle whose hypotenuse is 5. So we are meeting the Pythagorean theorem again, and of course Fermat's theorem as well, but in the case $n = 2$ in which solutions are possible.

Euler's *Algebra* offers two methods of solution, of which I present the first. One sets

$$\sqrt{x^2 + 1} = x + p,$$

and tries to find p, or rather x and p. Squaring, we obtain

$$x^2 + 1 = x^2 + 2xp + p^2 \Longleftrightarrow 1 = 2xp + p^2.$$

The second equation yields

$$x = \frac{1 - p^2}{2p}.$$

Thus if $p = m/n$,

$$x = \frac{n^2 - m^2}{2mn}$$

and

$$x^2 + 1 = \frac{n^4 - 2n^2m^2 + m^4}{4n^2m^2} + 1 = \left(\frac{n^2 + m^2}{2mn}\right)^2.$$

Euler gives a brief list of possibilities:

n	2	3	3	4	4	5	5	5	5
m	1	1	2	1	3	1	2	3	4
x	$\frac{3}{4}$	$\frac{4}{3}$	$\frac{5}{12}$	$\frac{15}{8}$	$\frac{7}{24}$	$\frac{12}{5}$	$\frac{21}{20}$	$\frac{8}{15}$	$\frac{9}{40}$

He also observes that the solution leads to an infinite number of Pythagorean triangles, thus to an infinite number of integral solutions of the equation

$$p^2 + q^2 = r^2.$$

He just takes

$$p = 2mn, \quad q = n^2 - m^2, \quad r = n^2 + m^2.$$

There are several other equations whose integral solutions Euler discusses. Although not immediately pertinent to us, it is worthwhile to spend a little time with them. He deals with Pell's equation, which will reappear in exacerbated form as the theory of units when we return to Kummer and his treatment of Fermat's equation. He also deals with the search for rational solutions of certain equations which, in modern terminology, is the search for rational points on elliptic curves.

Since the Taniyama-Shimura-Weil conjecture, about which a number of you are curious, often provides, among other things, an effective method for establishing the existence of such points, Euler's chapters may serve as an introduction not to the modern statements themselves but to their meaning and purpose.

Pell's equation

Before I begin, I observe that Euler does use the term Pell's equation and that following him the term passed into general use, but that the equation itself was introduced by Fermat in 1657 as a problem to mathematicians in general and to several English mathematicians in particular. It was solved within little more than a year by Fermat himself and by the English mathematicians.

If n is an integer and not 0, it is not possible for $n^2 + 1$ to be a square of a rational number, for that rational number would—if taken positive—have to be an integer larger than n, thus of the form $n + m$ and $(n + m)^2 = n^2 + 2mn + m^2$ is certainly larger than $n^2 + 1$ because $2mn$ and m^2 are both at least 1. On the other hand it might be possible for $an^2 + 1$ to be a square, not of course if a is negative or itself a square, but otherwise. This is the question investigated by Euler in Chapter 7 of II.2.

He begins his investigation with the following remark, in which one sees the name Pell mistakenly appearing.

> *Hiezu hat ein gelehrter Engländer, Namens Pell, eine sehr sinnreiche Methode erfunden, welche wir hier erklären wollen. Dieselbe ist nicht so beschaffen, daß sie auf allgemeine Art für jede Zahl a, sondern nur für jeden besondern Fall gebraucht werden kann.*

The last remark is more important to us than the reference to Pell. The method is a general method, but as a number-theoretic method and not an algebraic method; it is applied to an individual equation to obtain an answer. There is no general algebraic formula.

Suppose we want $2n^2 + 1$ to be the square. If it is the square of some number, that number can be taken to be positive and it will necessarily be larger than n. Write it as $n + p$. Then

$$2n^2 + 1 = n^2 + 2pn + p^2 \Longleftrightarrow n^2 = 2np + p^2 - 1.$$

This is a quadratic equation for n that can be solved to give

$$n = p \pm \sqrt{p^2 - (1 - p^2)} = p \pm \sqrt{2p^2 - 1}.$$

This number is only good to us if $2p^2 - 1$ is a square. One possibility is $p = 1$. This leads to $n = 0$, which is uninteresting or $n = 2$ and then

$$2n^2 + 1 = 9 = 3^2.$$

This example was so easy, although we applied the general method, that we try another, again taken from Euler's *Algebra*. We want to find an integral solution of $13n^2 + 1 = m^2$. One possibility is $n = 0$, $m = 1$, but we are looking for solutions of more interest.

Since $9n^2 < m^2 < 16n^2$, we conclude that $m = 3n + p$ with $p < n$, so that

$$13n^2 + 1 = 9n^2 + 6np + p^2 \Longleftrightarrow 4n^2 - 6pn - p^2 + 1 = 0.$$

Thus

$$n = \frac{6p \pm \sqrt{36p^2 - 16(1-p^2)}}{8} = \frac{3p \pm \sqrt{13p^2 - 4}}{4}.$$

We have to choose the +-sign. It is clear from this that $n > 6p/4$ and that $n < 7p/4$ so that $2p > n > p$ and therefore $n = p + q$, with $q < p$.

Continuing, we see that

$$n - \frac{3p}{4} = \frac{\pm\sqrt{13p^2 - 4}}{4}$$

or

$$p + 4q = \pm\sqrt{13p^2 - 4}.$$

Squaring, we obtain

$$p^2 + 8pq + 16q^2 = 13p^2 - 4 \Longleftrightarrow 12p^2 - 8pq - 16q^2 - 4 = 0.$$

The last equation can be divided by 4; the result is

$$3p^2 - 2pq - 4q^2 - 1 = 0.$$

We could decide to give these calculations up, fearing that they would continue forever, except that q is positive and smaller than p which is in turn smaller than n. Since these numbers are growing smaller and smaller, we will be forced to stop sooner or later. So we continue.

$$p = \frac{2q \pm \sqrt{4q^2 + 12(4q^2 + 1)}}{6} = \frac{q \pm \sqrt{13q^2 + 3}}{3}.$$

We might be tempted to try $q = 1$ here, so that $p = (q \pm 4q)/4$. With either sign, p is not integral, so that we have to continue.

Once again, we have to take the positive root if p is to be larger than q. Then $5q/4 > p > 4q/4$, so that $p = q + r$ with $r < q$. Thus $q = r + s$ with $s < r$. We continue and we now continue more rapidly, observing that we have at each stage to take the positive square root.

$$\begin{array}{lll}
p = q + r; & q + r = \dfrac{q + \sqrt{13q^2 + 3}}{3}; & q = \dfrac{2r + \sqrt{13r^2 - 3}}{3} \\
q = r + s; & r + s = \dfrac{2r + \sqrt{13r^2 - 3}}{3}; & r = \dfrac{s + \sqrt{13s^2 + 4}}{4} \\
r = s + t; & s + t = \dfrac{s + \sqrt{13s^2 + 4}}{4}; & s = 3t + \sqrt{13t^2 - 1} \\
s = 6t + u; & 6t + u = 3t + \sqrt{13t^2 - 1}; & t = \dfrac{3u + \sqrt{13u^2 + 4}}{4} \\
t = u + v; & u + v = \dfrac{3u + \sqrt{13u^2 + 4}}{4}; & u = \dfrac{v + \sqrt{13v^2 - 3}}{3} \\
u = v + x; & v + x = \dfrac{v + \sqrt{13v^2 - 3}}{3}; & v = \dfrac{2x + \sqrt{13x^2 + 3}}{3}
\end{array}$$

At this point, we can observe that $x = 1$ makes $13x^2 + 3$ a square and that it makes v integral, namely $v = 2$. Euler takes the process two steps further. If $v = 2$

then

$$\begin{aligned} u &= v + x = 3, \\ t &= u + v = 5, \\ s &= 6t + u = 33, \\ r &= s + t = 33 + 5 = 38, \\ q &= r + s = 38 + 33 = 71, \\ p &= q + r = 71 + 38 = 109, \\ n &= p + q = 109 + 71 = 180, \\ m &= 3n + p = 540 + 109 = 649. \end{aligned}$$

Thus

$$13n^2 + 1 = 421201 = 649^2.$$

We could perhaps take x larger, but not smaller, since $x = 0$ does not make $13x^2 + 3$ a square. In other words, we may very well not have found all solutions. This is indeed so. It is worthwhile to look more carefully at these calculations and to see how we might find others.

We continue Euler's calculations. He writes

$$v = x + y, \qquad x + y = \frac{2x + \sqrt{13x^2 + 3}}{3}, \qquad x = \frac{y + \sqrt{13y^2 - 4}}{4}$$

$$x = y + z, \qquad y + z = \frac{y + \sqrt{13y^2 - 4}}{4}, \qquad y = 3z + \sqrt{13z^2 + 1}$$

At this point, we are free to take the trivial solution that we earlier rejected, namely $z = 0$, which yields $y = 1$ and then $x = 1$ as before.

This leads, as we know, to the solution $n = 180$, $m = 649$, but now we can start with this value of n, taking it for z. This gives the following results.

$$\begin{aligned} y &= 1189, \\ x &= y + z = 1189 + 180 = 1369, \\ v &= x + y = 1369 + 1189 = 2558, \\ u &= v + x = 2558 + 1369 = 3927, \\ t &= u + v = 3927 + 2558 = 6485, \\ s &= 6t + u = 6 \times 6485 + 3927 = 42837, \\ r &= s + t = 42837 + 6485 = 49322, \\ q &= r + s = 49322 + 42837 = 92159, \\ p &= q + r = 92159 + 49322 = 141481, \\ n &= p + q = 141481 + 92159 = 233640, \\ m &= 3n + p = 3 \times 233640 + 141481 = 842401. \end{aligned}$$

Then

$$13n^2 + 1 = 709639444801 = m^2.$$

So we have found another solution. We could continue!

Before returning to Fermat's equation, I pass to Euler's next chapter, which is entitled *Von der Art, wie die Irrationalformel* $\sqrt{a + bx + cx^2 + dx^3}$ *rational gemacht*

wird. In other words, he wants to find solutions of the equation

$$y^2 = a + bx + cx^2 + dx^3. \tag{D}$$

We can take a, b, c and d to be integral, and we might at first look for integral solutions, but as Euler quickly explains, this turns out to be too difficult, and we had best content ourselves with rational solutions, and even they are difficult to find. It is useful to cite Euler's introduction to this chapter, because there is a great difference, or so it seems to me, between the present status of these problems and their status in the middle of the eighteenth century and much of the difference is the result of developments in the twentieth century, largely but not entirely in the second half. Conjectures, some, like the Taniyama-Shimura-Weil conjecture, proved, others, like the Birch-Swinnerton-Dyer conjecture, only partially established provide ways to decide, with the help of a computer, but the computer is not the essential ingredient, whether a given equation (D) has a solution, especially whether it has an infinite number of solutions. This was not the situation in which Euler found himself.

> *Es soll also die Formel $a + bx + cx^2 + dx^3$ zu einem Quadrate gemacht, und zu diesem Zwecke geiegnete Werthe für x in Rationalzahlen gesucht werden. Denn da dies schon weit größeren Schwierigkeiten unterworfen ist, so erforert es auch weit mehr Kunst, nur gebrochene Zahlen für x zu finden, und man ist genötight sich damit zu begnügen, une keine Auflösung in ganzen Zahlen zu verlangen. Von vorn herein ist auch hier zu bemerken, daß man keine allgemeine Auflösung geben kann, wie eben geschehen, sondern jede Operation giebt uns nur einen einzigen Werth für x zu erkennen, während die oben gebrauchte Methode auf einmal zu unendlich vielen Auflösungen führt.*

Basically Euler is reduced to guessing. He considers for example

$$y^2 = 1 + 3x^3.$$

He observes that $x = 0$, $x = 1$ and $x = 2$ yield three possibilities, with $y = 1$, $y = 2$ and $y = 5$.

Then he begins the search for more. Since $x = 1$ is a possibility, he suggests starting from this possibility, setting $x = 1 + z$ and trying to make $1 + 3x^3$ the square of $2 + pz$. Thus

$$4 + 4pz + p^2z^2 = (2 + pz)^2 = 1 + 3(1 + z)^3 = 1 + 3 + 9z + 9z^2 + 3z^3.$$

so he takes $p = 9/4$, leaving

$$\frac{81}{16}z^2 = 9z^2 + 3z^3.$$

Dividing both sides by z^2, we obtain

$$3z = \frac{81}{16} - 9 = \frac{63}{16}$$

so that

$$x = 1 - \frac{21}{16} = -\frac{5}{16} \quad y = 2 - \frac{9}{4}\frac{21}{16} = \frac{128 - 189}{64} = -\frac{61}{64}.$$

Then

$$1 + 3x^3 = 1 - \frac{375}{4096} = \frac{3721}{4096} = y^2.$$

One example suffices for our purposes!

$$x^3 + y^3 = z^3$$

Euler begins his discussion of the impossibility of solving this equation with all three of the integers x, y and z different from 0 with an attempt to apply the various techniques developed in the previous chapters, None succeed.

If x and y have a common divisor d, that number divides z as well, and we might as well replace x by x/d, y by y/d and z by z/d and thus suppose that any two of the three numbers x, y and z are relatively prime. In particular, at least one is odd; and if one is odd, then two are odd. Since, for example, $x^3 + y^3 = z^3$ implies that $x^3 + (-z)^3 = (-y)^3$, we might as well suppose, changing the labels if necessary, that x and y are odd. We next set

$$p = \frac{x+y}{2}, \quad q = \frac{x-y}{2},$$

so that

$$x = p + q, \quad y = p - q.$$

As a result one of p and q must be even and the other odd.

Then $x^3 + y^3$ is

$$(p+q)^3 + (p-q)^3 = p^3 + 3p^2q + 3pq^2 + q^3 + p^3 - 3p^2q + 3pq^2 - q^3 = 2p(p^2 + 3q^2).$$

If this is a cube, it is certainly even—as we already arranged—and thus divisible by 8, so that either p is even or $p^2 + 3q^2$ is divisible by 4. Since one of p and q is even and the other odd, only the first possibility is tenable. Thus 4 divides p and

$$\frac{p}{4}(p^2 + 3q^2)$$

is a cube. These two factors are relatively prime unless 3 divides p. At this point, the argument branches, according as 3 does not divide p or it does.

First case: 3 does not divide p

If it does not, then $p/4$ is a cube and so is $p^2 + 3q^2$. This means, or meant for Euler, but it is a point to which we shall have to return, that

$$p + q\sqrt{-3} = (t + u\sqrt{-3})^3.$$

We had shown, following Euler that if p and q were chosen such that this were true, thus if $p = t^3 - 9tu^2 = t(t^2 - 9u^2)$ and $q = 3t^2u - 3u^3 = 3u(t^2 - u^2)$, then $p^2 + 3q^2$ would be a cube. Since p and q are relatively prime, so are t and u.

Since q is odd, u is odd and t even. Since $p/4$ is a cube, so is

$$2p = 2t(t^2 - 9u^2) = 2t(t - 3u)(t + 3u)$$

Now I observe, and that is the essence of the case we are treating, that 3 does not divide the even number t because it does not divide p. Consequently these three numbers are relatively prime and all three all cubes. Thus

$$t + 3u = f^3, \quad t - 3u = g^3, \quad 2t = h^3,$$

and

$$f^3 + g^3 = h^3.$$

At this point, Euler argues as follows.

> *Wenn es also zwei solche Kuben in den größten Zahlen gäbe, so könnte man auch in viel kleineren Zahlen ebenfalls derartige angeben, deren Summe auch ein Kubus wäre, und in solcher Art könnte man auf immer kleinere derartige Kuben kommen. Da es nun in kleinen Zahlen derartige Kuben gewiss nicht giebt, so sind sie auch in den aller größten nicht möglich. Dieser Schluß wird dadurch bestätigt, daß auch der andere Fall eben dahin führ, wie wir sogleich sehen werden.*

We look a little closer at this argument, in particular at the other case, for, if we are not careful, our argument may simply be that if the first case occurs then so does the second, but with smaller triples, and there may be no reason whatsoever that this cannot occur. After looking at the other case, we look more carefully to see in what sense the numbers are becoming smaller.

Second case: 3 divides p

Suppose that 3 divides p, so that $p = 3r$ and

$$\frac{3r}{4}(9r^2 + 3q^2) = \frac{9r}{4}(3r^2 + q^2) \tag{E}$$

is a cube. The number r is also even, so that $3r^2 + q^2$ is divisible neither by 2 nor by 3. Consequently the two factors of (E) are relatively prime and both cubes. Thus

$$q = t(t^2 - 9u^2), \quad r = 3u(t^2 - u^2).$$

Because q is odd, t must be odd and u even. In addition, $9r/4$ is a cube and so is

$$\frac{8}{27}\frac{9r}{4} = \frac{2r}{3} = 2u(t^2 - u^2) = 2u(t + u)(t - u).$$

Once again, the three numbers $2u$, $t + u$, and $t - u$ are relatively prime, so that each is again a cube.

$$t + u = f^3, \quad t - u = g^3, \quad 2u = h^3, \quad h^3 = f^3 - g^3 = f^3 + (-g)^3.$$

What we have left to do is to assure ourselves that in both cases, we have succeeded in finding solutions that are definitely smaller. Since none of the three new numbers is 0, this cannot go on forever, so that we eventually reach a contradiction.

Are the solutions smaller?

In both the first and second case, the new numbers f and g are odd, so that the even number is still the one that stands by itself on one side of the equation. It is enough to verify that this even number is growing smaller, for that will lead to the same contradiction.

Recall that in the first case,

$$z^3 = 2p(p^2 + 3q^2) = 2p(p^2 + 3q^2) = f^3g^3h^3(t^2 + 3u^2)^3,$$

so that

$$z = \pm fgh(t^2 + 3u^2).$$

Sign aside, z is certainly larger than h because, signs again aside, f and g are both at least 1 and $t^2 + 3u^2$ is at least 3.

In the second

$$\begin{aligned} z^3 &= 2p(p^2+3q^2) = 18r(3r^2+q^2) \\ &= 54u(t+u)(t-u)(t^2+3u^2)^3 \\ &= 27f^3g^3h^3(3r^2+q^2)^3, \end{aligned}$$

so that

$$z = \pm 3fgh(3r^2+q^2).$$

Once again, h has to be smaller than z.

Lecture 5 [Lecture 13]

Preparation for Kummer

As preparation for the general theory, I present a version of Euler's proof that is formulated within the domain $\mathbf{Z}(\alpha)$. This version is presented in several texts on number theory, no doubt in an effort to introduce the student to more advanced methods. I leave it to you to judge whether it is more or less comprehensible. It is, however, essential that it be comprehended for it is nothing but Kummer's proof in a special and simple case.

The element in Euler's proof that is still missing becomes here the statement that every number ξ in $\mathbf{Z}(\alpha)$ is a product $\epsilon\pi_1^{a_1}\pi_2^{a_2}\cdots$. The number ϵ is a unit, π_1 and π_2, and so on are essentially different primes, that is one is not obtained from another by multiplication with a unit. Moreover, this factorization is essentially unique. All others are obtained by multiplying each π_i by a unit ϵ_i, thus changing them in an inessential manner, and modifying ϵ as required.

For example, we have seen that $1+9\alpha$ and $3+11\alpha$ are primes. Then

$$\xi = -80+19\alpha = (1+9\alpha)(3+11\alpha) = \epsilon(-9-8\alpha)(-3-11\alpha), \qquad \epsilon = -\alpha^2$$

because

$$\alpha(1+9\alpha) = -9-8\alpha, \qquad \alpha\alpha^2 = 1.$$

The presence of the units is a nuisance, about which there is nothing to be done. We take the (essentially) unique factorization for granted for the moment. It will be treated later. I observe immediately that it is the failure of unique factorization in the domains $\mathbf{Z}(\alpha)$ when

$$\alpha = \cos(2\pi/p) + i\sin(2\pi/p),$$

p being not 3 but a larger prime number, for example 23, that creates the initial bewilderment and forces the introduction of *ideal numbers*.

We shall prove a stronger statement than that of Fermat, namely that there is no solution of

$$\xi^3+\eta^3+\zeta^3 = 0, \qquad \xi\eta\zeta \neq 0$$

in $\mathbf{Z}(\alpha)$. If any two of these numbers were divisible by a prime π then all three would be, and we could divide by it. So we may as well assume, when proving the theorem, that any two have no common divisor.

For convenience, I now introduce a modern notation. If ξ and η are two numbers in $\mathbf{Z}(\alpha)$ and ζ a third, then

$$\xi \equiv \eta \pmod{\zeta}$$

means that $\xi-\eta$ is a multiple of ζ. Recall that $\lambda = 1-\alpha$ is a prime and that $3 = \rho\lambda^2$, where ρ is a unit.

Date of lecture: Spring term, February 29, 2000.

Statement 1. *If ω is not divisible by λ then*

$$\omega^3 \equiv \pm 1 \pmod{\lambda^4}$$

If $\omega = a + b\alpha$, then $\omega + b\lambda = a + b$, so that

$$\omega \equiv a + b \pmod{\lambda}.$$

Since 3 is also a multiple of λ and any integer n is of the form $m + 3r$, $m = 0, \pm 1$, we may take $\omega \equiv 0, \pm 1 \pmod{\lambda}$. By hypothesis, 0 is excluded, and that leaves ± 1.

If the statement is true for ω then it is certainly true for $-\omega$ and conversely. Thus, multiplying ω by -1 if necessary, we suppose that $\omega \equiv 1 \pmod{\lambda}$ or that

$$\omega = 1 + \beta\lambda.$$

Then

$$\begin{aligned}\omega^3 - 1 &= (\omega - 1)(\omega - \alpha)(\omega - \alpha^2) \\ &= \beta\lambda(\beta\lambda + 1 - \alpha)(\beta\lambda + 1 - \alpha^2) \\ &= \beta\lambda^3(\beta + 1)(\beta - \alpha^2).\end{aligned}$$

Since

$$\alpha^2 = \alpha^2 - 1 + 1 \equiv 1 \pmod{\lambda},$$

the number

$$\beta(\beta + 1)(\beta - \alpha^2) \equiv \beta(\beta + 1)(\beta - 1)$$

is divisible by λ.

Statement 2. *If $\xi^3 + \eta^3 + \zeta^3 = 0$, then one of ξ, η, ζ is divisible by λ.*

If not, then

$$0 = \pm 1 \pm 1 \pm 1 \pmod{\lambda^4}.$$

Thus, either

$$\pm 1 \equiv 0 \pmod{\lambda^4}$$

or

$$\pm 3 \equiv 0 \pmod{\lambda^4}.$$

The first possibility is certainly out of the question. The second possibility is out of the question because 3 is equal to a unit times λ^2 and thus not a multiple of λ^4—because of unique factorization!

Suppose then that $\xi^3 + \eta^3 + \zeta^3 = 0$ and that λ divides ζ, so that

$$\zeta = \lambda^n\gamma,$$

where $n > 0$ and where λ does not divide γ. So we are to prove the impossibility of

$$\xi^3 + \eta^3 + \lambda^{3n}\gamma^3 = 0, \tag{A}$$

in which neither ξ nor η is divisible by λ and in which the greatest common divisor of $\xi \neq 0$ and $\eta \neq 0$ is 1. As is often the case in mathematics, it is better to prove a stronger assertion, the impossibility under the same conditions of

$$\xi^3 + \eta^3 + \epsilon\lambda^{3n}\gamma^3 = 0, \tag{B}$$

where ϵ is a unit. This we prove with two assertions.

Statement 3. *If* (B) *is satisfied with the conditions specified then $n > 1$.*

Statement 4. *If* (B) *is possible with the conditions specified for a given* $n = m > 1$, *then it is possible for* $n = m - 1$.

The first of these statements is easy to verify. (B) means that

$$-\epsilon\lambda^{3n}\gamma^{3n} \equiv \pm 1 \pm 1 \pmod{\lambda^4}$$

The signs cannot be the same because λ does not divide 2. (Otherwise its norm could not be 3.) Thus we have

$$-\epsilon\lambda^{3n}\gamma^{3n} \equiv 0 \pmod{\lambda^4}.$$

This requires that $3n \geqslant 4$ or that $n > 1$.

It is the final statement that is difficult to prove. Its proof exploits a very important technique in number theory, that of descent. We show that when a statement is true for one number, then it is true for a smaller number, and continue in this way until we reach a very small number for which we easily show it is impossible. This technique, introduced by Fermat, remained until recently the most powerful one available.

We begin by factoring.

$$-\epsilon\lambda^{3m}\gamma^3 = \xi^3 + \eta^3 = (\xi + \eta)(\xi + \alpha\eta)(\xi + \alpha^2\eta). \tag{C}$$

Just to be certain, we explicitly verify the second equation by expanding the right-hand side.

$$\xi^3 + \xi^2\eta(1 + \alpha + \alpha^2) + \xi\eta^2(1 + \alpha + \alpha^2) + \eta^3 = \xi^3 + \eta^3.$$

The differences of the terms on the left side of (C) are $\eta\lambda$, $\alpha\eta\lambda$, $\alpha^2\eta\lambda$, all associates of $\eta\lambda$. Thus each of them is divisible by λ but not by λ^2, because λ does not divide η. One of the three factors on the left of (C) must be divisible by λ^2 because $m \geqslant 2$. Since we can replace η by $\alpha\eta$ or by $\alpha^2\eta$ without changing (B), thereby permuting the three factors on the left of (C), we might as well suppose that $\xi + \eta$ is divisible by λ^2. The other factors are then divisible by λ but not by λ^2.

So we express these factors as follows.

$$\xi + \eta = \lambda^{3m-2}\kappa_1, \quad \xi + \alpha\eta = \lambda\kappa_2, \quad \xi + \alpha^2\eta = \lambda\kappa_3, \tag{D}$$

in which none of κ_1, κ_2 and κ_3 is divisible by λ.

We have next to verify that these three numbers, κ_1, κ_2 and κ_3 are relatively prime to each other. Observe that

$$\lambda(\kappa_2 - \kappa_3) = \alpha(1 - \alpha)\eta = \alpha\lambda\eta,$$
$$\lambda(\alpha\kappa_3 - \alpha^2\kappa_2) = \alpha\xi - \alpha_2\xi = \alpha\lambda\xi$$

or cancelling the λ,

$$\kappa_2 - \kappa_3 = \alpha\eta,$$
$$\alpha\kappa_3 - \alpha^2\kappa_2 = \alpha\xi,$$

so that any divisor of κ_2 and κ_3 is also a divisor of η and ξ and must therefore be a unit. Consequently κ_2 and κ_3 are relatively prime.

In the same way,

$$\lambda(\kappa_3 - \lambda^{3m-3}\kappa_1) = \alpha^2\lambda\eta,$$
$$\lambda(\kappa_3 - \alpha^2\lambda^{3m-3}\kappa_1) = -\alpha^2\lambda\eta,$$

so that, cancelling the λ, we see that κ_1 and κ_3 must be relatively prime. A similar calculation will show that κ_1 and κ_2 have to be relatively prime.

We substitute (D) in (C). The result is

$$-\epsilon\gamma^3 = \kappa_1\kappa_2\kappa_3.$$

When we factor each of κ_1, κ_2 and κ_3 as well as γ and γ^3 into a product of primes and remember that if a prime factor appears, for example, in κ_1 then it cannot appear in κ_2 or in κ_3, then we see that every prime factor that appears in κ_1 appears to a power that is a multiple of 3.

$$\kappa_1 = \epsilon_1\pi_1^{3a_1}\pi_2^{3a_2}\cdots = \epsilon_1\theta^3, \qquad \theta = \pi_1^{a_1}\pi_2^{a_2}\cdots. \tag{E}$$

For similar reasons,

$$\begin{aligned}\kappa_2 &= \epsilon_2\phi^3,\\ \kappa_3 &= \epsilon_3\psi^3.\end{aligned} \tag{F}$$

We substitute (E) and (F) in (D). The result is

$$\xi + \eta = \epsilon_1\lambda^{3m-2}\theta^3, \quad \xi + \alpha\eta = \epsilon_2\lambda\phi^3, \quad \xi + \alpha^2\eta = \epsilon_3\lambda\psi^3.$$

Consequently

$$\begin{aligned}0 &= (1+\alpha+\alpha^2)(\xi+\eta)\\ &= \xi + \eta + \alpha(\xi+\alpha\eta) + \alpha^2(\xi+\alpha^2\eta)\\ &= \epsilon_1\lambda^{3m-2}\theta^3 + \epsilon_2\alpha\lambda\phi^3 + \epsilon_3\alpha^2\lambda\psi^3.\end{aligned} \tag{G}$$

If we cancel a λ from the right-hand side of (G), then we are almost back to an equation of the form (B), but with m replaced by $m-1$ and that was our goal. To be precise, we have

$$\phi^3 + \epsilon_4\psi^3 + \epsilon_5\lambda^{3m-3}\theta^3 = 0, \qquad \epsilon_4 = \epsilon_3\alpha/\epsilon_2, \quad \epsilon_5 = \epsilon_1/\epsilon_2\alpha.$$

This is at first sight not quite right, because of the ϵ_4.

The process is completed as follows. As $m \geqslant 2$,

$$\phi^3 + \epsilon_4\psi^3 \equiv 0 \pmod{\lambda^2}.$$

We had already seen that

$$\phi^3 \equiv \pm 1 \pmod{\lambda^2}, \quad \psi^3 \equiv \pm 1 \pmod{\lambda^2}.$$

Indeed the λ^2 can even be replaced by λ^4. Thus

$$\pm 1 \pm \epsilon_4 \equiv 0 \pmod{\lambda^2}.$$

There are six choices for ϵ_4, either ± 1, $\pm\alpha$ or $\pm\alpha^2$. The first is fine, for we just replace ψ by $\pm\psi$ and the ϵ_4 is absorbed. On the other hand,

$$\pm(1+\alpha) = \mp\alpha^2, \quad \pm(1-\alpha) = \pm\lambda,$$

and

$$\pm(1+\alpha^2) = \mp\alpha, \quad \pm(1-\alpha^2) = \mp\alpha^2\lambda,$$

so that these numbers are either units or associates of λ. Consequently $\epsilon_4 = \pm 1$.

Lecture 6 (and Lecture 8) [Lecture 14 (and Lecture 16)]

Final stages

We are in the middle of two proofs of the impossibility of solving Fermat's equation for $n = 3$. To complete the classical proof, we need to establish with Euler that if an integer $p^2 + 3q^2$ is a cube, then

$$p + q\sqrt{-3} = (t + u\sqrt{-3})^3.$$

To complete the proof in the style of Kummer, we need to show that there is unique factorization into primes in the domain $\mathbf{Z}(\alpha)$.

Although more abstract, it is easier; so I begin with the proof of unique factorization. It employs a variant of Euclid's algorithm that I prove, taking advantage of a certain modern freedom and informality, pictorially. I begin with the representation of the numbers of $\mathbf{Z}(\alpha)$ as complex numbers in the plane. These are then the numbers of the form

$$a + b\alpha = (a - b/2) + ib\sqrt{3}/2.$$

When represented in the plane, they form a regular triangular lattice as in Figure 1. One point and the six adjacent points are shown in Figure 1a. If for example, the point is $(0, 0)$, then the neighboring points are $(1/2 + i\sqrt{3}/2)$, $(-1/2 + i\sqrt{3}/2)$, -1, $-1/2$, $-i\sqrt{3}/2$, $(1/2 - i\sqrt{3}/2)$. These are in fact the points $\cos(2k\pi/6) + i\sin(2k\pi/6)$, $k = 0, \ldots, 5$ and thus all at a distance 1 from $(0, 0)$. They are the 6th roots of unity.

If instead of all the numbers in $\mathbf{Z}(\alpha)$ we consider those that are multiples of some other ξ, then we simply take this lattice and stretch and rotate it, because multiplying by a complex number amounts, as we saw to a stretching and a rotation. The points that are multiples of ξ are the vertices of the triangles in Figure 2. The sides of the new triangles will be the length L of ξ. I superimpose Figure 2 on Figure 1 obtaining Figure 3.

Suppose we have some other number η. It lies inside or on the boundary of one of the triangles. I look more carefully at this triangle or indeed at any equilateral triangle with vertices A, B and C as in Figure 4. The point D is in the center of the triangle. Suppose the side of the triangle has length L. Then the distance from D to any of the points A, B or C is $L/\sqrt{3}$. Thus the distance of the point A to any point of the small triangle in Figure 4 that contains it is at most $L/\sqrt{3}$. We return to Figure 3 and to an arbitrary number η in the domain $\mathbf{Z}(\alpha)$. It is contained in one of the triangles of the figure (imagined as extending off to infinity), thus in one of the three smaller triangles into which that triangle is divided as in Figure 5.

Date of lecture: Spring term, March 7 (and 21), 2000.

In other words it lies at a distance at most $L/\sqrt{3}$ from one of the vertices. If this vertex is $\zeta\xi$ then the length of $\eta - \zeta\xi$ is at most $L/\sqrt{3}$.

In other words, if we start from ξ and η, we can perform the same sequence of operations as in Euclid. We take η to have the larger distance from 0, thus the larger length and the larger norm as the norm is the square of the length. Then we subtract an appropriate multiple of ξ from η. The result μ has a length smaller than ξ. We begin again with the pair μ and ξ, subtracting an appropriate multiple of μ from ξ to obtain a number ν with length smaller than μ. Continuing in this way we eventually arrive at 0. Therefore the penultimate number, the one δ reached immediately before 0, divides all the immediate ones and is the greatest common divisor of ξ and η.

Expressed in another way, the collection of all numbers $\beta\xi + \gamma\eta$ with β and γ in the domain $\mathbf{Z}(\alpha)$ is just the collection of multiples of δ, the collection $\beta\delta$ with β in the domain $\mathbf{Z}(\alpha)$. This δ may not be unique. If there were another δ', we would have

$$\delta' = \beta\delta, \quad \delta = \beta'\delta',$$

but then

$$\beta\beta' = 1$$

and both β and β' are units. Thus, up to a unit, the greatest common divisor of ξ and η is well-defined.

We then show, just as in the modern treatment of Proposition 30 of Book VII and its consequences, that every number of $\mathbf{Z}(\alpha)$ is a product of primes in an essentially unique way.

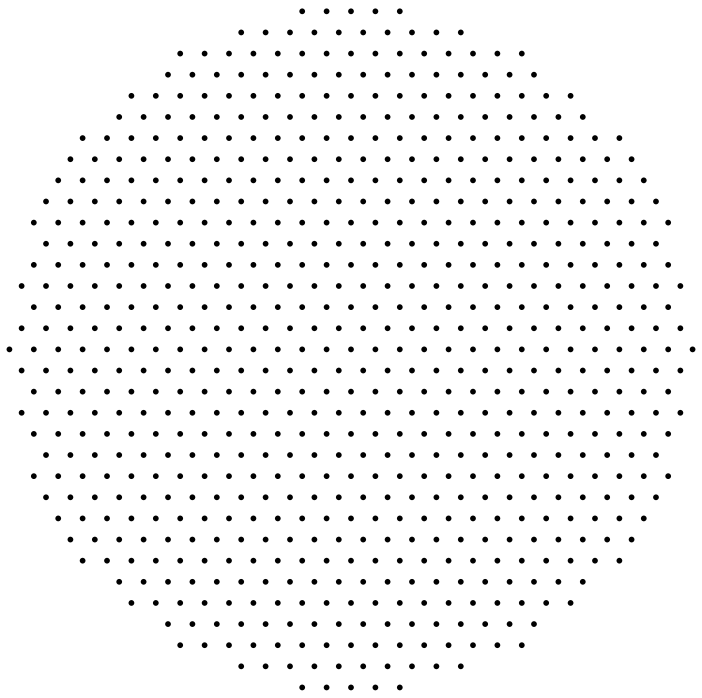


Figure 1

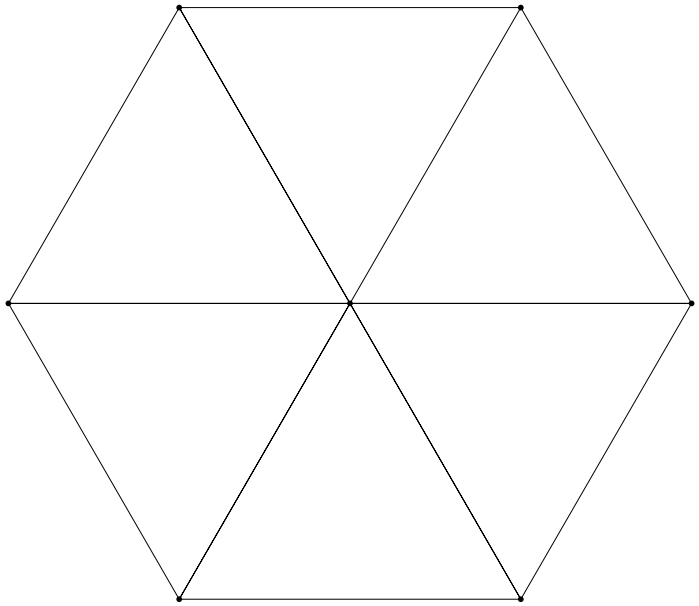


Figure 1a

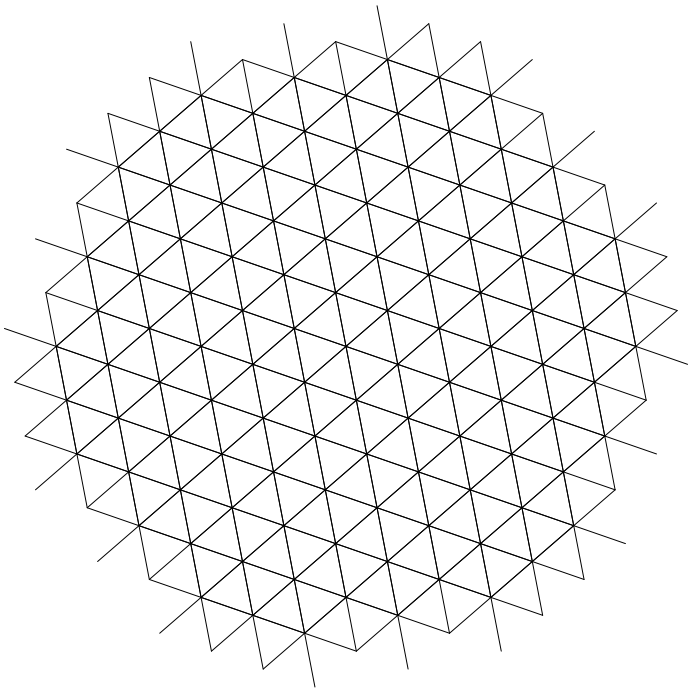


Figure 2

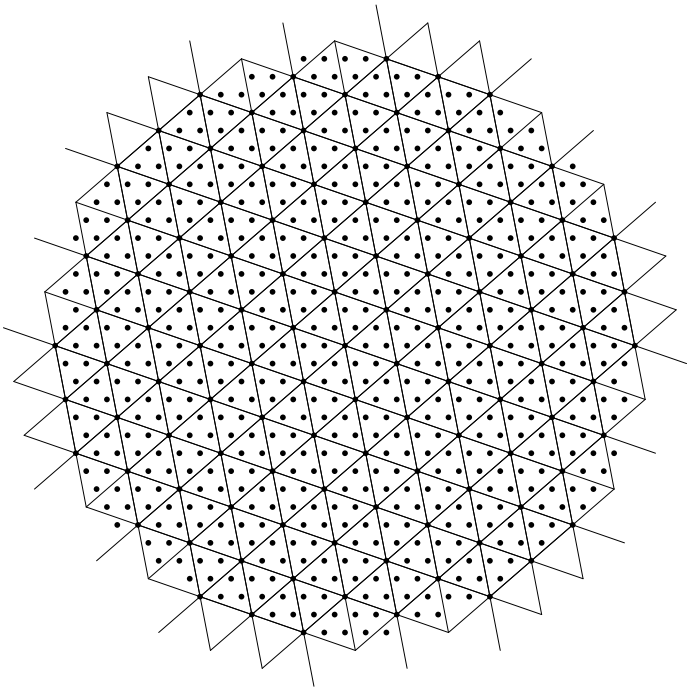


Figure 3

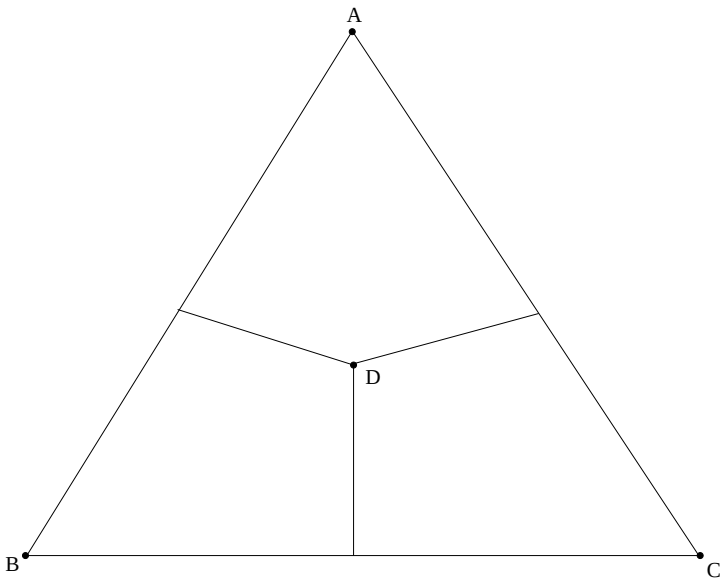


Figure 4

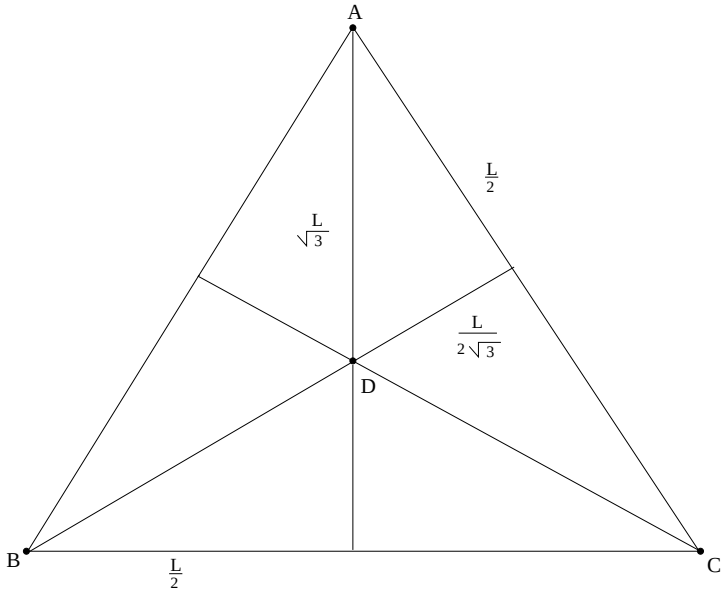


Figure 5

Completion of Euler's argument

Recall what was missing from our argument. We needed to show that if a^2+3b^2, with a and b relatively prime, was a cube then we could find t and u such that $a = t^3 - 9tu^2$, $b = 3t^2u - 3u^3$. Thus

$$\begin{aligned} a^2 + 3b^2 &= (t^3 - 9tu^2)^2 + 3(3t^2u - 3u^3) \\ &= t^6 - 18t^4u^2 + 81t^2u^4 + 27(t^4u^2 - 2t^2u^4 + u^6) \\ &= t^6 + 9t^4u^2 + 27t^2u^4 + 27u^6 \\ &= (t^2 + 3u^2)^3. \end{aligned}$$

The pertinent argument appears in the Memoirs of the Saint Petersburg Scientific Academy for 1760 (vol. 1.II of Euler's *Opera omnia*). Those who read Latin, even if with difficulty, are advised to turn directly to the paper itself, which contains nothing but the argument about to be presented. The discussion of Euler could not be more leisurely.

There is, however, one thing that we need to know that is not in the paper itself. So I begin with it. I fix a prime p. We want to consider integers, but we do not want to distinguish between two whose difference is a multiple of p. Thus we only need consider the integers $0, 1, 2, \dots, p-1$ because any integer positive or negative is equal to one of these numbers plus a multiple of p.

$$-14 = 3 + (-1)17, \quad 103 = 1 + 6 \times 17, \quad 212 = 8 + 12 \times 17.$$

We use the symbol $a \equiv b \pmod{p}$ to mean that $a-b$ is a multiple of the prime p. If the prime is understood, we write $a \equiv b$. We are here dealing with a basic notion of number theory. If a and b are not equal to 0 modulo p, then, by Proposition VII.30, neither is ab. Thus if $ab \equiv ac$ or $ab - ac \equiv 0$, then $a(b-c) \equiv 0$ and $b - c \equiv 0$ or $b \equiv c$. Starting from a which is not equivalent to 0 modulo p, we form a^2, a^3, a^4 and so on. Since modulo p there are only $p-1$ possibilities—except for 0—there will be a repetition.

$$a^m \equiv a^n, \qquad n > m, \quad a \not\equiv 0.$$

Then

$$a^m(a^{n-m} - 1) \equiv 0 \implies a^{n-m} \equiv 1.$$

Cautionary remarks

When I first turned to this aspect of Euler's argument, I was persuaded that Weil's reconstructions in his book *Number Theory* would convince me that the necessary materials for a complete proof were in Euler. I am no longer so sure. Certainly only details are missing and these details, although they require fastidious care, are not difficult, but even Weil's arguments seem to me at times to be just a little too facile. Providing all the details is time-consuming and they are of little or no interest to a general audience, so that, even though I include it in the notes, I shall omit from the lectures a great deal of the material that follows.

Thus for each a there is a smallest positive integer r that depends on a and is such that $a^r \equiv 1$. If $a^s \equiv 1$ and $s > r$ then, by the euclidean algorithm $s = mr + n$, $0 \leqslant n < r$, and then $1 \equiv a^s \equiv a^{rm}a^n \equiv a^n$, so that $n = 0$. We refer to this number r as the order of a modulo p. This order has already played an important role in our discussion of Gauss's periods. For $p = 17$, the order of 2 is 8 and that of 3 is 16. Notice that if a^s is any power of a then we can always find a t such that $s + t$ is

divisible by r and then $a^{s+t} \equiv 1$. So $a^s a^t \equiv 1$. For example $8 \equiv 2^3 \pmod{17}$ and $3+5$ is divisible by 8. Thus if we multiply 8 by $32 = 2^5$ we obtain $256 = 1 + 15 \times 17$.

The powers 2^n, $n = 1, \dots, 16$ are

$$2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536.$$

Taken modulo 17, they become

$$2, 4, 8, 16, 15, 13, 9, 1, 2, 4, 8, 16, 15, 13, 9, 1.$$

We see that they repeat themselves with a period 8 so that 2 has the order 8 modulo 17.

The powers 3^n, $n = 1, \dots, 16$ are

$$3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049,$$
$$177147, 531441, 1594323, 4782969, 14348907, 43046721.$$

Taken modulo 17, they are

$$3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1.$$

We exploited this without discussing congruences in our discussion of Gauss's periods.

Both examples suggest that the order of any integer a modulo p always divides $p-1$. To verify this we let a be any integer not divisible by p and r its order. I first observe that if b and c are two other integers not divisible by p, then the residues modulo p of the two collections

$$b, ab, a^2 b, \dots, a^{r-1} b.$$
$$c, ac, a^2 c, \dots, a^{r-1} c$$

are either exactly the same or completely different.

Consider for example $a = 12$, $p = 29$. Then

$$a^2 \equiv 28, \quad a^3 \equiv 17, \quad a^4 \equiv 1,$$

so that the order of 12 modulo 29 is 4. Then

$$\{2, 12 \times 2, 28 \times 2, 17 \times 2\} = \{2, 24, 27, 5\},$$
$$\{3, 12 \times 3, 28 \times 3, 17 \times 3\} = \{3, 7, 26, 22\},$$
$$\{5, 12 \times 5, 28 \times 5, 17 \times 5\} = \{5, 2, 24, 27\}.$$

Thus if $b = 2$ and $c = 5$, the two collections are the same, but if $b = 2$ and $c = 3$, they are completely disjoint.

The proof proceeds by observing that if $a^m b = a^n c$ and, for example, $n \geqslant m$ then $a^m(a^{n-m}c - b) \equiv 0$, so that $a^{n-m} c \equiv b$. Thus the residue of b is in the collection for c and so is that of $a^s b$ for any s.

This means that $\{1, 2, \dots, p-1\}$ is obtained as the union of various collections

$$\{c, ac, a^2 c, \dots, a^{r-1} c\}$$

(all numbers being taken modulo p,) each with r elements. In other words, in Euclid's language, r measures $p-1$ or, in ours, r divides $p-1$. For example, if $p = 17$ and $a = 2$ then

$$\{1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7\} = \{1, 2, 4, 8, 16, 15, 13, 9\},$$
$$\{3, 2 \cdot 3, 2^2 \cdot 3, 2^3 \cdot 3, 2^4 \cdot 3, 2^5 \cdot 3, 2^6 \cdot 3, 2^7 \cdot 3\} = \{3, 6, 12, 7, 14, 11, 5, 10\},$$

and these two sets together make up

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}.$$

There is another important point. For any p, we can always find an a whose order is exactly $p-1$. For $p = 17$, we used without much comment that one such a was $a = 3$. We can get by with a slightly weaker statement.

Let p be given. There is no integer m dividing $p-1$ except $p-1$ itself such that $a^m \equiv 1 \pmod{p}$ for all a not dividing p.

If this were so then every a would be a solution of

$$x^m - 1 \equiv 0 \pmod{p}.$$

Then, by long division of polynomials but only modulo p,

$$x^m - 1 \equiv (x-1)(x^{m-1} + cx^{m-2} + dx^{m-3} + \cdots) + f,$$

but we must have $f \equiv 0$. Continuing and dividing by $x-2$, then by $x-3$ and so on, we finally arrive at

$$x^m - 1 \equiv (x-1)(x-2)(x-3)\cdots(x-m).$$

If $m \neq p-1$, we substitute $x = m+1$ and arrive at a contradiction.

To what use does Euler put this conclusion? He proves the following assertion.

Suppose p is given and p leaves the remainder 1 upon division by 6. Then there is a pair of relatively prime integers a and b such that $a^2 + 3b^2$ is divisible by p.

Since p cannot be 2, it must be odd. Suppose that $f^2 + fg + g^2$ is divisible by p but not by p^2. Replacing f by $f + p^2$ or g by $g + p^2$ if necessary, we may suppose that f and g are both odd. Then

$$f^2 + fg + g^2 = \left(\frac{f-g}{2}\right)^2 + 3\left(\frac{f+g}{2}\right)^2,$$

so that it is enough to show that we can find f and g relatively prime and such that p divides $f^2 + fg + g^2$.

I observe in passing that we can then arrange that p divides $f^2 + fg + g^2$ but that p^2 does not. For if p^2 divides this expression, then

$$(f \pm p)^2 + (f \pm p)g + g^2 = f^2 + fg + g^2 + (\pm 2f + p \pm g)p$$

will for one of the two signs not be divisible by p^2 unless p divides $2f + g$, but that is excluded by hypothesis.

The assumption is that $p = 6n+1$ because it leaves the remainder 1 on division by 6. Consider the identity,

$$a^{6n} - 1 = (a^{2n} - 1)(a^{4n} + a^{2n} + 1).$$

The left side is divisible by p if a is not. Moreover we can choose an a such that $a^{2n} - 1$ is not divisible by p. As a result, we can find an a such that $a^{4n} + a^{2n} + 1$ is divisible by p. So we take $f = a^{2n}$ and $g = 1$.

Our major task now is to deduce from this that if $p = 6n+1$ then we can always find a pair of relatively prime integers a and b such that $a^2 + 3b^2 = p$.

We first deduce this from unique factorization in the domain $\mathbf{Z}(\alpha)$, because the argument will explain some of Kummer's calculations, and only afterwards return

to Euler's, and therefore presumably also Fermat's, more elementary arguments. Choose f and g such that

$$\mathrm{N}(f - g\alpha) = f^2 + fg + g^2$$

is divisible by p but not by p^2. Consider the greatest common divisor η of p and $\xi = f - g\alpha$. It cannot be 1 because the norm of any number $\mu p + \nu\xi$ is equal to

$$\mu\overline{\mu}p^2 + p\mu\overline{\nu}\overline{\xi} + \nu\overline{\nu}\,\mathrm{N}\,\xi$$

and is therefore divisible by p. In particular $\mathrm{N}\,\eta$ is divisible by p. But $\mathrm{N}\,\eta$ divides $\mathrm{N}\,p = p^2$. So $\mathrm{N}\,\eta = p$. Thus $\eta = k + \ell\alpha$ and

$$k^2 - k\ell + \ell^2 = p.$$

There are 12 numbers with this property $\epsilon\eta$ and $\epsilon\overline{\eta}$, if ϵ is any unit. We have

$$\alpha\eta = \alpha(k + \ell\alpha) = -\ell + (k - \ell)\alpha,$$
$$\alpha^2\eta = \alpha^2(k + \ell\alpha) = (\ell - k) - k\alpha.$$

Since p is odd, either k or ℓ is odd. Thus either they are both odd or one is odd and one is even. Thus of the three numbers η, $\alpha\eta$ and $\alpha^2\eta$, exactly one

$$\zeta = c + 2b\alpha = (c - b) + b\sqrt{-3} = a + b\sqrt{-3}, \qquad a = c - b,$$

in which the coefficient of α is even. This is then also true of $-\zeta$, $\overline{\zeta}$ and $-\overline{\zeta}$ which equal

$$-a - b\sqrt{-3}, \quad a - b\sqrt{-3}, \quad -a + b\sqrt{-3}.$$

Moreover

$$p = \mathrm{N}(a + b\sqrt{-3}) = a^2 + 3b^2.$$

Replacing if necessary, ζ by one of the other three numbers, we can even arrange that a and b are positive. So there seems to be an essentially unique way to represent a prime p of the form $6n + 1$ as $a^2 + 3b^2$ with a and b positive.

Interjection

At this point, we should tie up some loose ends and clarify the argument on the previous page, as it contains a gap. Dividing a number n by 6 leaves the remainder 0, 1, 2, 3, 4 or 5. If n leaves the remainder 1 upon division by 3 then it must leave the remainder 1 or 4 upon division by 6 and if it is a prime, then it must leave the remainder 1 for otherwise it would be even. Thus every prime p that is congruent to 1 modulo 3 can be represented as

$$\mathrm{N}\,\eta = \eta\overline{\eta}, \qquad \eta = k + \ell\alpha.$$

We saw some time ago that η and $\overline{\eta}$ could not differ by multiplication by a unit. Thus they are relatively prime, so that p is indeed the product of two relatively prime numbers η and $\overline{\eta}$ in the domain $\mathbf{Z}(\alpha)$. Consequently p can be represented in a unique way as $a^2 + 3b^2$.

Interjection continued

We have discovered three kinds of primes in $\mathbf{Z}(\alpha)$: the prime λ; the ordinary primes 2, 5, 11 that are congruent to 2 modulo 3 and that, therefore, continue to be prime in $\mathbf{Z}(\alpha)$; and those primes ξ such that $\mathrm{N}\,\xi$ is a prime congruent to 1 modulo 3. These are, up to multiplication by a unit, the only primes.

If ξ is a prime then $\xi\bar{\xi} = \mathrm{N}\,\xi$ is a number n that admits a factorization

$$n = p_1^{a_1} p_2^{a_2} \cdots$$

and each p_i admits a factorization that involves only the three kinds of primes just described. Thus so does n. Since the factorization of n is unique, ξ is equal to a unit times one of those primes.

We now, following Euler, attempt to show this directly, starting from the fact that we can find a pair of relatively prime integers c and d such that p divides $c^2 + 3d^2$.

An important step is the observation that if we have such a c and d, then we can find c_1 and d_1 such that $c_1 = kp \pm c$ and $d_1 = \ell p \pm d$, with $-p/2 < c_1, d_1 < p/2$. All we do is to lay the multiples of p out on the line and to choose the ones kp and ℓp that are closest to c and d. Since the distance between adjacent multiples is p, the closest multiple to, for example, c has to be at a distance at most $p/2$ from it. It cannot be exactly at a distance $p/2$ because $p/2$ is not an integer. Since

$$c_2 + 3d_1^2 = c^2 + d^2 \pm 2c_1 kp \pm 6d_1 \ell p + k^2 p^2 + 3\ell^2 p^2$$

differs from $c^2 + 3d^2$ by a multiple of p, we might as well suppose that $-p/2 < c, d < p/2$. Then

$$N = c^2 + 3d^2 < \frac{p^2}{4} + 3\frac{p^2}{4} = p^2,$$

so that N/p is smaller than p.

Notice that

$$(x^2 + 3y^2)(u^2 + 3v^2) = (xu \pm 3yv)^2 + 3(xv \mp yu)^2, \tag{A}$$

so that if we can represent M and N as the sum of a square and 3 times a square then we can so represent MN.

Suppose that

$$N = c^2 + 3d^2, \qquad N < p^2. \tag{B}$$

It may happen that N is even, a disagreeable possibility. But then c and d are both odd. Moreover $4 = 1^2 + 3 \cdot 1^2$. We apply (A).

$$4N = (c \pm 3d)^2 + 3(c \mp d)^2. \tag{C}$$

If 4 divides $c + d$ then it also divides $c - 3d$ and we choose $c_2 = (c - 3d)/4$, $d_2 = (c + d)/4$. Otherwise 4 divides $c - d$ and $c + 3d$ and we choose $c_2 = (c + 3d)/4$ and $d_2 = (c - d)/4$. The equation (C) becomes

$$\frac{N}{4} = c_2^2 + 3d_2^2.$$

Thus 4 divides N and $N/4 < p^2$ has a representation of the type (B). We replace N by $N/4$. The new N is odd because $c_2 - d - 2$ is either $-d$ or d and thus odd. So we suppose in addition that N is odd.

If 3 divides N then 3 divides c and

$$\frac{N}{3} = c_2^2 + 3d_2^2, \quad c_2 = d, \quad d_2 = \frac{c}{3}.$$

So we remove 3 from N. The result is not divisible by 3, because c and d are relatively prime.

Suppose some other odd prime q divides N. It then divides neither c nor d. Moreover q divides $4c^2 + 12d^2$. Set $y = 2d$, $x = c - d$. Then

$$x^2 + xy + y^2 = (c-d)^2 + (c-d)2d + 4d^2 = c^2 + 3d^2$$

is divisible by q. So is

$$x^3 - y^3 = (x-y)(x^2 + xy + y^2).$$

Moreover q cannot divide both x and y. So it can divide neither. Choose z such that $zy \equiv 1 \pmod{q}$. Then if $w = zx$,

$$w^3 - 1 \equiv (zx)^3 - (zy)^3 \equiv z^3(x^3 - y^3) \equiv 0 \pmod{q}.$$

Finally, w is not equivalent to 1 modulo q, for if it were then x would be equivalent to y and

$$x^2 + xy + y^2 \equiv 3x^2 \pmod{q},$$

So the left side would not be divisible by q. The order of w is therefore 3 and 3 must therefore divide $q - 1$. Since q is odd it must leave the remainder 1 on division not only by 3 but also by 6.

$$6k + r = 3(2k) + r, \qquad r = 1, 4.$$

If $r = 4$ then $6k + r = 2(3k + 2)$ is even.

Penultimate step

We now want to show that every prime that leaves the remainder 1 on division by 6 can be represented as $a^2 + 3b^2$ with a and b necessarily relatively prime. We have seen that this is so for the prime 7 and some other small primes. If it is not generally true, then there is certainly a smallest prime p for which it is false. This could be p. Then we find an N smaller than p^2 which can be represented as $c^2 + 3d^2$. If $N = p$, there is nothing to do, but if N is larger than p, we have to make it smaller—and smaller—until it is equal to p. If N is not p, then $N/p < p$ is divisible by a prime q and that prime is necessarily smaller than p. Consequently, by assumption, $q = x^2 + 3y^2$ and

$$qN = (c^2 + 3d^2)(x^2 + 3y^2) = (cx \pm 3dy)^2 + 3(cy \mp dx)^2. \tag{D}$$

None of the numbers c, d, x and y is divisible by q, because both q and N are divisible by q and c is relatively prime to d and x to y. Moreover

$$c^2 + 3d^2 \equiv x^2 + 3y^2 \equiv 0.$$

Thus

$$3c^2y^2 \equiv 3d^2x^2 \iff cy \equiv \pm dx.$$

Changing the sign of one of the numbers if necessary, we arrange that $cy - dx$ is divisible by q. Then

$$dy(cx + 3dy) \equiv d^2x^2 + 3d^2y^2 \equiv d^2(x^2 + 3y^2) \equiv 0.$$

So we can divide (D) by q^2, obtaining

$$\frac{N}{q} = c_1^2 + d_1^2, \quad c_1 = \frac{cx + 3dy}{q}, \quad d_1 = \frac{cy - dx}{q}.$$

So we have succeeded in replacing N by N/q, thereby making it smaller.

A property of relatively prime numbers that needs to be mentioned

Suppose that a and b are relatively prime. Then there are two numbers k and ℓ such that $ka + \ell b = 1$. Suppose some number d divides the two numbers ac and bc, so that $ac = md$ and $bc = nd$. Then

$$c = (ka + \ell b)c = kac + \ell bc = kmd + \ell nd = (km + \ell n)d$$

is divisible by d.

Final step

The final step is in fact composed of several small steps and a large digression. I want to show first of all that, if N is any positive number that leaves the remainder 1 upon division by 6, then the number of representations of N in the form $c^2 + 3d^2$ with a and b positive and relatively prime is $2^{\rho-1}$ if ρ is the number of different prime divisors of N. For example $343 = 7^3$ has exactly one and $57967 = 7^3 \cdot 13^2$ has two.

Digression

We vacillate between two methods, that of Euler (perhaps even Fermat) and one based on later considerations of Kummer (perhaps even Gauss). Euler's method demands that we demonstrate more, in particular an assertion that I now explain. We say that a number N is properly represented as $c^2 + 3d^2$ if c and d are relatively prime and positive. We know that a number N not divisible by 2 or by 3 has a proper representation exactly when all of its prime divisors leave the remainder 1 upon division by 6.

Why? Suppose N has such a representation,

$$N = c^2 + 3d^2.$$

If p divides N and $b = 2d$, $a = c - d$, then

$$a^2 + ab + b^2 = (c - d)^2 + 2(c - d)d + 4d^2 = c^2 + 3d^2.$$

Moreover the only common divisor of a and b could be 2. Finally

$$a^3 - b^3 = (a - b)(a^2 + ab + b^2)$$

is divisible by p and $a - b$ is not, for if it were then

$$a^2 + ab + b^2 \equiv 3a^2 \pmod{p},$$

would not be divisible by p. (If p divided a, it would then also have to divide b.) We can find an e such that $eb \equiv 1 \pmod{p}$ and then

$$0 \equiv e^3(a^3 - b^3) \equiv f^3 - 1 \pmod{p}, \qquad f = ea$$

and, at the same time, f is not equivalent to 1 modulo p. As a consequence, the order of f modulo p is 3 and 3 divides $p-1$. Thus p leaves the remainder 1 upon division by 3 and therefore, as it is odd, the remainder 1 upon division by 6.

On the other hand, suppose that

$$N = p_1^{m_1} p_2^{m_2} p_3^{m_3} \cdots p_\rho^{m_\rho}$$

and that each

$$p_i = \pi_i \overline{\pi}_i$$

is the product of two conjugate primes in $\mathbf{Z}(\alpha)$. We can even suppose that

$$\pi_i = c_i + d_i\sqrt{-3}, \quad \overline{\pi}_i = c_i - d_i\sqrt{-3}.$$

Consider then

$$\xi = \pi_1^{m_1}\pi_2^{m_2} \cdots = c + d\sqrt{-3}.$$

Its norm is

$$c^2 + 3d^2 = (\mathrm{N}\,\pi_1)^{m_1}(\mathrm{N}\,\pi_2)^{m_2}(\mathrm{N}\,\pi_3)^{m_3} \cdots = N. \tag{E}$$

On the other hand it is not divisible by any ordinary prime because an ordinary prime is either a prime in $\mathbf{Z}(\alpha)$ or has as prime factors both π and $\overline{\pi}$, π being a prime of $\mathbf{Z}(\alpha)$, and no such pairs appear in (E). Thus c and d are relatively prime.

At each i there are four choices. We can replace c_i and d_i by their negatives $-c_i$ and $-d_i$, which has little effect on the final result. Both c and d are also replaced by their negatives. On the other hand, we can leave c_i alone and replace d_i by $-d_i$, thus replacing ξ_i by $\overline{\xi}_i$, which is prime to it. This leads, because of unique factorization, to a completely different number ξ. Ignoring signs, we obtain 2^ρ different numbers ξ, thus 2^ρ ways of representing N as $c^2 + 3d^2$. If we change all of the ξ_i to $\overline{\xi}_i$, the result is to replace ξ by $\overline{\xi}$, thus to replace d by $-d$. In conclusion, we see that only $2^{\rho-1}$ of the representations will have both c and d positive.

Further cautionary remarks

On turning, finally, to Legendre's argument in his *Théorie des nombres* it appears at first that we could have stopped here if, instead of using Euler's initial argument, we had used the variant of it found there. Curiously enough, although still in the classical mode, thus still working with ordinary integers and not with surds of any kind, it is closer to Kummer's arguments. It appears that all we need know is that an odd number N not divisible by 3 can be represented as

$$N = a^2 + 3b^2$$

if and only all its prime divisors leave the remainder 1 upon division by 6. On closer examination, however, Legendre's argument (4th edition, vol. II, pp. 357–360) seems to suffer from the same defect as Euler's.

It runs as follows. Since one of the three numbers in Fermat's equation

$$x^3 + y^3 = z^3$$

is necessarily even, we suppose it to be z and write $z = 2^m u$, with u odd. Then

$$(x+y)(x^2 - xy + y^2) = 2^{3m}u^3.$$

Legendre next attempts to establish the important fact that u is necessarily divisible by 3. Suppose not.

Since

$$x^2 - xy + y^2 = (x+y)^2 - 3xy,$$

the only possible common divisor of $x+y$ and $x^2 - xy + y^2$ is 3. x and y are then odd, but as u is supposed not to be divisible by 3, this is out of the question. Thus $x+y$ and $x^2 - xy + y^2$ are both cubes. Moreover $x+y$ is even and $x^2 - xy + y^2$ is odd. Let

$$\left(\frac{x+y}{2}\right)^2 + 3\left(\frac{x-y}{2}\right)^2 = x^2 - xy + y^2 = \sigma^3.$$

Since σ^3 can be represented as the sum of a square and 3 times a square so can σ because they have the same prime divisors. Thus

$$\sigma = f^2 + 3g^2.$$

Thus if

$$F = f(f^2 - 9g^2), \quad G = 3g(f^2 - g^2), \tag{A}$$

then

$$\sigma^3 = F^2 + 3G^2.$$

Legendre then, unfortunately, concludes that

$$\frac{x+y}{2} = F, \quad \frac{x-y}{2} = G, \tag{B}$$

a completely unwarranted conclusion, because if σ is composite there are several ways of representing it as the sum of a square and 3 times a square. This error is repeated later in the argument. To correct the argument, it is necessary to show, and for that the following discussion is necessary, that f and g can be so chosen that both (A) and (B) are satisfied.

Euler's argument

Euler's argument seems to require that he show directly that if N is a number all of whose prime divisors leave the remainder 1 upon division by 6 and ρ is the number of distinct prime divisors of N, then the number of proper representations of N in the form $c^2 + 3d^2$ is $2^{\rho-1}$. We have seen that this can be established as a consequence of unique factorization in the domain $\mathbf{Z}(\alpha)$. How can it be established directly?

I begin with an earlier formula. Suppose

$$M = a^2 + 3d^2, \quad N = c^2 + 3d^2.$$

Then

$$MN = (a^2 + 3b^2)(c^2 + 3d^2) = (ac \pm 3bd)^2 + 3(ad \mp bc)^2 = e^2 + 3f^2.$$

where

$$e = ac \pm 3bd \quad f = ad \mp bc,$$

the signs being chosen consistently, either $+$ in the first and $-$ in the second or $-$ in the first and $+$ in the second. I suppose that both M and N leave the remainder 1 upon division by 6.

Then

$$\begin{aligned} ae \mp 3bf &= a(ac \pm 3bd) \mp 3b(ad \mp bc) = a^2c + 3b^2c = Mc, \\ af \pm be &= a(ad \mp bc) \pm b(ac \pm 3bd) = a^2d + 3b^2d = Md. \end{aligned} \tag{F}$$

As a result any number that divides both e and f divides M. The same argument with c and d replacing a and b shows that it also divides N. Thus if M and N are relatively prime, then e and f are relatively prime.

To remove any possible doubt that the same argument applies, I write out the analogue of (F) in which M is replaced by N.

$$\begin{aligned} ce + df &= c(ac \pm 3bd) + 3d(ad \mp bc) = ac^2 + 3ad^2 = aN, \\ \mp cf \pm de &= \mp c(ad \mp bc) \pm (d)(ac \pm 3bd) = bc^2 + 3bd^2 = bN. \end{aligned} \tag{G}$$

Notice that if

$$ae - 3bf, \quad af + be$$

are both divisible by M then

$$ae + 3bf, \quad af - be$$

are not both divisible by M, for then M would divide $2ae$ and $2af$, and therefore, being odd, a. It would also divide $3bf$ and be and thus e and thus $3b$ and therefore b as M is prime to 3. Thus the signs appearing in (F) are determined; there is no choice and we can recover c and d from e and f. Changing the sign of both e and f changes the sign of c and d. Changing the sign of just one forces us to modify the choice of signs in (F) and causes the sign of either c or d to change.

Since the signs of both e and f can be changed, this yields eight representations of MN as $e^2 + 3f^2$, of which only two will have e and f positive. If

$$M = p_1^{a_1} \cdots p_\sigma^{a_\sigma}$$

has σ distinct prime factors and

$$N = p_1^{b_1} \cdots p_\tau^{b_\tau}$$

has τ, then MN has $\rho = \sigma + \tau$ and from each of the

$$2^{\sigma-1}2^{\tau-1} = 2^{\sigma+\tau-2} = 2^{\rho-2}$$

representations of M together with N we obtain 2 of MN, leading to $2 \cdot 2^{\rho-2} = 2^{\rho-1}$ representations of MN. Thus, if the assertion to be proved is valid for M and N, then it is true for their product.

As a consequence, if we can show that for a power p^m of a prime that leaves the remainder 1 upon division by 6, there is exactly one proper representation $p = c^2 + 3d^2$ with c and d positive, we will be done, because then the assertion is true for p^m and any of our numbers N is a product $p^m M$ with $M = 1$ or with p and M relatively prime, and with M smaller than N. Thus if the assertion is true for M, it is true for N and we can work our way down.

Let p be such a prime. We first show, repeating an argument, that p has a unique representation with c and d positive. Suppose

$$p = a^2 + 3b^2, \quad p = c^2 + 3d^2.$$

Then, as in formula (D),

$$p^2 = (ac \pm 3bd)^2 + 3(ad \mp bc)^2 = e^2 + 3f^2. \tag{H}$$

We can arrange, by the same argument as before, that p divides $ad - bc$, although this may require changing the sign of d. But then p divides not only $f = ad - bc$, but also $ac + bd$. This can only be so if $ad = bc$ and $ac + 3bd = p$. Since a, b and c are still positive, d must also be positive. Since $a : c = b : d$ and both a and b

and c and d are relatively prime, we conclude from Euclid's Proposition VII.21, or otherwise, that $a = c$, $b = d$.

On the other hand, if we take $a = c$, $b = d$ in (H), we obtain

(I) $$p^2 = (c^2 - 3d^2)^2 + 3(2cd)^2 = e^2 + 3f^2, \qquad e = \pm(c^2 - 3d^2), \quad f = 2cd.$$

Since one of c and d must be odd and the other even, and since 3 does not divide c, $e = \pm(c^2 - 3d^2)$ and $f = 2cd$ are relatively prime. Choosing the sign correctly, we arrange that both e and f are positive.

Conversely, if

(J) $$p^2 = e^2 + 3f^2,$$

then

$$p^3 = (ce \pm 3df)^2 + 3(cf \mp de)^2 = a^2 + 3b^2, \qquad a = ce \pm 3df, \quad b = cf \mp de.$$

Once again, one choice of sign leads to p dividing b and therefore also a and the second leads to a representation of p^3 by relatively prime a and b.

Choose, however, the sign for which p divides $cf \mp de$ and therefore also $ce \pm 3df$. Then we obtain

$$p = \left(\frac{ce \pm 3df}{p}\right)^2 + 3\left(\frac{cf \mp de}{p}\right)^2.$$

Since there is only one representation of p, we conclude that

(K) $$ce \pm 3df = \pm pc, \quad \pm cf - de = \pm pd,$$

where the signs on the right are, at first, independent of each other and of those on the left. On the left, they are the same.

Set $f' = \pm f$, so that (K) becomes

(L) $$ce + 3df' = \pm pc, \quad cf' - de = \pm pd.$$

Multiply the first of these equations by d and the second by c and add to obtain

$$pf' = 3d^2 f' + c^2 f' = \pm pdc \pm pcd.$$

Since $f' \neq 0$, the two signs on the right must be the same and $f' = \pm 2cd$. Multiplying the equations (L) by c and $3d$ and subtracting, we obtain

$$pe = c^2 e + 3d^2 e = \pm pc^2 \mp 3pd^2 = \pm p(c^2 - 3d^2),$$

as the signs on the right are the same. Thus the possible new solutions (J) are in fact the same as those deduced from (I).

At this point we have found that there is at least one proper, positive representation of p^m for $m = 1, 2, 3$ and exactly one if $m = 1, 2$. The argument, however, clearly allows us to pass to higher and higher powers of m and to establish this in general.

At last

Recall what we needed to establish to complete Euler's argument. We had a number

$$M = c^2 + 3d^2$$

although we were then following Euler, using p or q for c and q or r for d. This number was a cube $M = N^3$ and c and d were relatively prime. We needed to write

(M) $$c = t(t^2 - 9u^2), \quad d = 3u(t^2 - u^2).$$

The signs are not important here, changing the sign of t changes that of u and changing the sign of u changes that of d.

Suppose that $M = p^{3m}$ and $N = p^m$. If

$$N = t^2 + 3u^2$$

then, as we have seen, we can construct a representation of N^2 as

$$N^2 = (t^2 - 3u^2) + 3(2tu),$$

and this representation, apart from the determination of sign, is unique.

We construct a representation of N^3 as

$$N^3 = \Big(t(t^2 - 3u^2) \pm 6tu^2\Big)^2 + 3\Big(t(2tu) \mp u(t^2 - 3u^2)\Big)^2,$$

The second coefficient here is

$$2t^2u \mp (t^2u - 3u^3) = \begin{cases} u(t^2 + 3u^2) = pu \\ 3t^2u - 3u^3, \end{cases}$$

so that only the +-sign is permissible, and that yields

$$N^3 = \Big(t(t^2 - 3u^2)\Big)^2 + 3\Big(3u(t^2 - u^2)\Big)^2.$$

Since the positive proper representation of N^3 is unique, this is it and (M) is established.

To complete the argument, we proceed as usual, passing from smaller to larger N. Thus suppose $N = N_1N_2$, with N_1 and N_2 relatively prime. Then we have seen that any proper representation

$$N^3 = c^2 + 3d^2$$

is given, apart from signs, as

$$(c_1c_2 \pm 3d_1d_2)^2 + 3(c_1d_2 \mp d_1c_2)^2,$$

where $N_1 = c_1^2 + 3d_1^2$ and $N_2 = c_2^2 + 3d_2^2$ are proper representations of N_1 and N_2. Moreover the four possible choices of sign for c_1 and d_1 and the four for c_2 and d_2 yield exactly eight choices for c and d, as a simultaneous change of the signs of c_1, d_1, c_2 and d_2 has no effect on c and d. These eight results come as two sets of four, the values of c and d in one set being obtained by making all possible sign changes.

If

$$c_1 = t_1(t_1^2 - 9u_1^2), \quad d_1 = 3u_1(t_1^2 - u_1^2)$$

and

$$c_2 = t_2(t_2^2 - 9u_2^2), \quad d_2 = 3u_2(t_2^2 - u_2^2),$$

consider

$$t = t_1t_2 \pm 3u_1u_2, \quad u = t_1u_2 \mp t_2u_1.$$

Then $c_1c_2 \pm 3d_1d_2$ is equal to

$$t_1t_2(t_1^2 - 9u_1^2)(t_2^2 - 9u_2^2) \pm 27u_1u_2(t_1^2 - u_1^2)(t_2^2 - u_2^2) =$$
$$t_1t_2(t_1^2t_2^2 - 9t_1^2u_2^2 - 9t_2^2u_1^2 + 81u_1^2u_2^2) \pm 27u_1u_2(t_1^2t_2^2 - t_1^2u_2^2 - u_1^2t_2^2 + u_1^2u_2^2),$$

from which we remove the two terms $t_1^3t_2^3$ and $\pm 27u_1^3u_2^3$ to obtain

(N) $$t_1t_2(-9t_1^2u_2^2 - 9t_2^2u_1^2 + 81u_1^2u_2^2) \pm 27u_1u_2(t_1^2t_2^2 - t_1^2u_2^2 - u_1^2t_2^2).$$

On the other hand, $t^3 - 9tu^2$ is equal to

$$t_1^3 t_2^3 \pm 9t_1^2 t_2^2 u_1 u_2 + 27 t_1 t_2 u_1^2 u_2^2 \pm 27 u_1^3 u_2^3 - 9(t_1 t_2 \pm 3u_1 u_2)(t_1 u_2 \mp t_2 u_1)^2$$

from which we remove the same two terms to obtain

$$\pm 9t_1^2 t_2^2 u_1 u_2 + 27 t_1 t_2 u_1^2 u_2^2 - 9(t_1 t_2 \pm 3u_1 u_2)(t_1 u_2 \mp t_2 u_1)^2 =$$
$$\pm 9t_1^2 t_2^2 u_1 u_2 + 27 t_1 t_2 u_1^2 u_2^2 - 9(t_1 t_2 \pm 3u_1 u_2)(t_1^2 u_2^2 \mp 2t_1 t_2 u_1 u_2 + t_2^2 u_1^2).$$

This we separate into the terms with the arbitrary and those with no sign. The first are

$$\pm\Big(27 t_1^2 t_2^2 u_1 u_2 - 27(t_1^2 u_1 u_2^3 + t_2^2 u_1^3 u_2)\Big),$$

while the second are

$$27 t_1 t_2 u_1^2 u_2^2 - 9t_1^3 t_2 u_1^2 - 9 t_1 t_2^3 u_1^2 + 81 t_1 t_2 u_1^2 u_2^2.$$

They are the same as the terms in (N). We conclude that

$$c = c_1 c_2 \pm 3 d_1 d_2 = t(t^2 - 9u^2),$$

and this is one-half of what we want to show.

For the second half we calculate $c_1 d_1 \mp d_1 c_2$ and $3u(t^2 - u^2)$. The first is

$$3 t_1 u_2 (t_1^2 - 9u_1^2)(t_2^2 - u_2^2) \mp 3 t_2 u_1 (t_2^2 - 9u_2^2)(t_1^2 - u_1^2); \tag{O}$$

and the second

$$3(t_1 u_2 \mp t_2 u_1)\Big((t_1 t_2 \pm 3u_1 u_2)^2 - (t_1 u_2 \mp t_2 u_1)^2\Big). \tag{P}$$

With the wisdom of experience, we separate in both (O) and (P), the terms without an arbitrary sign from those with. Moreover, we discard the 3 that is common to all terms in both these expressions.

This is easy for (O) and leads to

$$t_1 u_2 (t_1^2 t_2^2 - t_1^2 u_2^2 - 9u_1^2 t_2^2 + 9u_1^2 u_2^2)$$

and to

$$t_2 u_1 (t_2^2 t_1^2 - t_2^2 u_1^2 - 9u_2^2 t_1^2 + 9u_2^2 u_1^2),$$

the second expression being obtained from the first by interchanging the indices 1 and 2.

For (P), there is more to sort out. The terms without the sign yield

$$t_1 u_2 (t_1^2 t_2^2 + 9u_1^2 u_2^2 - t_1^2 u_2^2 - t_2^2 u_1^2) - t_2 u_1 (6 t_1 t_2 u_1 u_2 + 2 t_1 u_2 t_2 u_1).$$

On collecting terms and rearranging, this becomes

$$t_1 u_2 (t_1^2 t_2^2 + 9u_1^2 u_2^2 - t_1^2 u_2^2 - 9t_2^2 u_1^2).$$

The terms with sign yield

$$t_1 u_2 (6 t_1 t_2 u_1 u_2 + 2 t_1 u_2 t_2 u_1) + (-t_2 u_1)(t_1^2 t_2^2 + 9u_1^2 u_2^2 - t_1^2 u_2^2 - t_2^2 u_1^2),$$

or

$$-t_2 u_1 (-8t_1^2 u_2^2 + t_1^2 t_2^2 + 9u_1^2 u_2^2 - t_1^2 u_2^2 - t_2^2 u_1^2),$$

which is

$$-t_2 u_1 (t_1^2 t_2^2 + 9u_1^2 u_2^2 - 9t_1^2 u_2^2 - t_2^2 u_1^2).$$

We conclude that

$$d = -3u(t^2 - u^2).$$

Since we are free to change the sign of u, this is sufficient for our purposes.

Two lives

Ernst Eduard Kummer (1810–1893)

Évariste Galois (1811–1832)


Galois 1848
A.G.

E. E. Kummer

Galois theory

Suppose we have an equation with rational coefficients

$$Z^n + a_1 Z^{n-1} + a_2 Z^{n-2} + \cdots + a_{n-2} Z^2 + a_{n-1} Z^1 + a_n = 0 \tag{A}$$

and that no factorization of

$$Z^n + a_1 Z^{n-1} + a_2 Z^{n-2} + \cdots + a_{n-2} Z^2 + a_{n-1} Z^1 + a_n$$

as

$$(Z^k + b_1 Z^{k-1} + \cdots + b_{k-1} Z^1 + b_k)(Z^\ell + c_1 Z^{\ell-1} + \cdots + c_{\ell-1} Z^1 + a_\ell),$$

with all the b_i and c_j also rational is possible. If such a factorization exists, then necessarily $k + \ell = n$.

The equation (A) will have n roots,

$$z_1, z_2, \ldots, z_n$$

Notice that if we have an expression

$$z_1^{m_1} z_2^{m_2} \cdots z_n^{m_n}$$

and if one of the m_i is larger than $n-1$, then we can use the relation

$$z_i^{m_i} = z_i^{m_i - n} z_i^n = -z_i^{m_i - n}(a_1 z_i^{n-1} + a_2 z_i^{n-2} + \cdots)$$

to replace it by a combination of terms that involve no power of z_i greater than $m_i - 1$. Thus all the numbers that can be obtained from $z_1, z_2, \ldots, z_n$ by multiplying them together, multiplying the results by fractions, and adding the results together can be expressed by a finite number of them.

An example well known to us is the equation

$$Z^n + Z^{n-1} + Z^{n-2} + \cdots + Z^2 + Z^1 + 1 = 0,$$

in which n is a prime. Its roots are

$$z_j = \cos(2\pi j/n) + i \sin(2\pi j/n), \qquad i = \sqrt{-1}, \quad j = 1, \ldots, n-1.$$

Since $z_j z_k = z_\ell$ if $\ell - j - k$ is divisible by n, the numbers obtained in the above way can all be expressed as

$$a_1 z_1 + a_2 z_2 + \cdots + a_{n-1} z_{n-1}.$$

In general, it is not possible to predict in advance the size of a collection of expressions $\{w_1, \ldots, w_N\}$ of this form such that any other can be expressed as

$$a_1 w_1 + a_2 w_2 + a_3 w_3 + \cdots + a_N w_N$$

The smallest possible size N is extremely important in Galois theory, because it is exactly the number of symmetries provided we include the trivial one. This is the basic theorem of the theory, a theory that sprung fully armed from the head of Galois.

Consider again our example. The number N is $n-1$. The symmetries were

$$z_1 \to z_1^k = z_k, \qquad k = 1, 2, \ldots, n-1.$$

This symmetry took $z_\ell = z_1^\ell$ to $(z_1^\ell)^k = z_1^{k\ell} = z_m$ if $m - k\ell$ is divisible by n. There are certainly N symmetries and we saw that there were no more, because z_1 has to go to a number with the same properties, thus to another root of

$$Z^{n-1} + Z^{n-2} + \cdots + Z + 1 = 0.$$

Thus in this case, we are familiar with the main theorem of Galois theory.

In general any two of the N symmetries can be multiplied together:

$$\rho : z_i \to \rho(z_i) = z_j,$$
$$\sigma : z_j \to \sigma(z_j) = z_k,$$
$$\tau = \sigma \circ \rho : z_i \to \tau(z_i) = z_k.$$

It is by no means always the case that $\sigma \circ \rho = \rho \circ \sigma$. One important symmetry is the one for which every root is its own reflection. We denote it ι. Associated to any symmetry ρ there is a reverse symmetry $\sigma = \rho^{-1}$.

$$\rho : z_i \to z_j,$$
$$\sigma : z_j \to z_i,$$
$$\sigma \circ \rho : z_i \to z_i.$$

This is usually expressed by saying that the symmetries form a group.

There are two other assertions of the Galois theory that it is worth mentioning. First of all, the only numbers with maximal symmetry, thus which remain unchanged no matter which symmetry is applied are the rational numbers, which form the *field* of reference. If the field of reference is changed, thus if for example the coefficients of the polynomials in question are arbitrary numbers of the form $a + b\alpha$, with a and b rational, then the symmetries are then symmetries that preserve all relations with coefficients from this field. The field is larger; therefore there are more constraints and fewer symmetries. The valid statements of the theory remain the same, but it has to be understood that in each of them there are more coefficients and fewer symmetries allowed!

Not knowing quite what to say about a single number, since a number has in itself almost no properties, all its properties being defined by its relations to other numbers, mathematicians attach a great deal of importance to the group of symmetries, calling it the Galois group. If you look carefully at various advanced theories, you will see that they all treat the group and that the roots themselves are largely—but not entirely—neglected. We shall return to some simple applications of the notion, but first we turn to Galois himself.

Lecture 7 [Lecture 15]

Historical background for Galois—from Enc. Brit. 11th ed.

It begins with the fall of the last Bourbon, Charles the tenth.

> The united opposition of monarchist Liberals and imperialist republicans responded by legal resistance, then by a popular *coup d'état*, to the ordinances of July 1830, which dissolved the intractable Chamber, eliminated licensed dealers from the electoral list, and muzzled the press. After fighting for three days against the troops feebly led by the Marmont of 1814, the workmen, driven to the barricades by the deliberate closing of Liberal workshops, gained the victory, and sent the white flag of the Bourbons on the road to exile.
>
> The rapid success of the 'Three Glorious Days' ('les Trois Glorieuses', as the July Days were called), put the leaders of the parliamentary opposition into an embarrassing position. While they had contented themselves with words, the small Republican-Imperialist party, aided by the almost entire absence of the army and police, and by the convenience which the narrow, winding, paved streets of those times offered for fighting, had determined upon the revolution and brought it to pass. But the Republican party, which desired to re-establish the Republic of 1793, recruited chiefly from among the students and workmen, and led by Godefroy Cavaignac, the son of a Conventionalist, and by the chemist Raspail, had no hold on the departments nor on the dominating opinion in Paris. Consequently this premature attempt was promptly seized upon by the Liberal *bourgeoisie* and turned to the advantage of the Orleanist party, which had been secretly organized since 1829 under the leadership of Thiers, with the *national* as its organ. Before the struggle was yet over, Benjamin Constant, Casimir Périer, Lafitte, and Odilon Barrot had gone to fetch the Duke of Orleans from Neuilly, and on receiving his promise to defend the Charter and the tricolor flag, installed him at the Palais Bourbon as lieutenant-general of the realm, while La Fayette and the Republicans established themselves at the Hôtel de Ville. An armed conflict between the two governments was imminent, when Lafayette (*there are two spellings of the name in the original*), by giving his support to Louis Philippe, decided matters in his favour.

Date of lecture: Spring term, March 14, 2000.

With this decision of Lafayette, the hopes of the republican students, among them Galois, were disappointed. The text continues at some length, but I content myself with some brief citations, just to capture the flavor of the subsequent two years.

> The liberal ideas of the son of Philippe Égalité, the part he had played at Valmy and Jemappes, his gracious manner and his domestic virtues, all united in winning Louis Philippe the good opinion of the public.
>
> But the tradition of France was both twofold and contradictory, *i.e.* the Catholic-legitimist and the revolutionary. Louis-Philippe had them both against him.
>
> Now Louis-Philippe, beneath the genial exterior of a bourgeois and peace-loving king, was entirely bent upon recovering his authority which was menaced from the very first on the one hand by the anger of the royalists at their failures, and on the other hand by the impatience of the republicans to follow up their victory.

Galois was one of the impatient republicans.

> The struggle against the republicans was still longer, for having lost all their chance of attaining power by means of the Chamber, they proceeded to reorganize themselves into armed secret societies.

To what extent the reorganization had begun by the time of Galois's death on May 31, 1832, I do not know.

Some dates in the life of Galois

October 18, 1811.	Born at Bourg-la-Reine, now in the suburbs of Paris.
1815.	His father elected mayor of Bourg-la-Reine.
1818–1823.	Learns latin from his mother.
1823.	Enters the royal college of Louis-le-Grand. Remains until 1829. Studies Latin, Greek, French, a brilliant student.
1827.	Introduced to mathematics through a text of Legendre, begins to study Lagrange.
1827–1828.	Fails to be accepted at the École Polytechnique.
1829.	First publication in April. Submits first memoirs to the Académie des Sciences in May and June. Father commits suicide in July. Enters the École Préparatoire, the name of the École Normale during the Restoration, in October.
1830.	Submits a second memoir—on conditions for the solvability of equations by radicals, to the Académie française in February. Learns in June of its loss. In December publishes a letter attacking the Director of the École Normale (which must have regained its old name after July) for his behavior during the Revolution. He is excluded from the school and the affair reaches the press.
1831.	In January publishes a letter *Lettre sur l'enseignement* on pedagogy, signed with initials, he is also formally expelled from

	the École. Submits once again, on the invitation of Poisson, a second memoir on the solution of equations by radicals to the Académie. On the recommendation of Poisson it will be declined on July 4. It will appear much later, long after his death.
May 9, 1831.	Revolutionary toast to Louis-Philippe—interpreted as a threat.
May 10, 1831.	Arrested.
June 15, 1831.	Acquitted.
July 14, 1831.	Arrested again during a republican demonstration on the Pont Neuf.
October 23, 1831.	Sentenced to six months imprisonment in Saint-Pélagie for possession of a weapon and for wearing the uniform of the forbidden Republican Artillery Guard. He will write a preface to his memoir there in December.
April 1832.	Released from prison. Appears to fall in love with the daughter of his landlord. So far as I know, his passion was not reciprocated, and her character appears to me to be somewhat doubtful.
May 29, 1832.	Challenged to a dual under obscure circumstances.
May 30, 1832.	The "duel" takes place. Galois has no second and is mortally wounded.
May 31, 1832.	Dies.

Two books

There are many. A recent one, with many references is by a mathematician Laura Toti Rigatelli, *Matematica sulle barricate*. It is available in English. There is of course also a great deal of information in Galois's *Écrits et Mémoires mathématiques*. A novel with the title *The French mathematician* is advertised in recent issues of the NY Review of Books. The blurb runs,

> This remarkable novel resurrects a young overemotional, impetuous, and headstrong genius whose personal failures read like a Hugo novel but whose voice resonates more clearly now with the passage of time.

It is clearly about Galois.

Extracts from Galois's writings
Two memoirs on pure analysis

Preface. First of all the second page of this work is not encumbered by the names, given names, qualities, dignities and praises of any avaricious prince whose purse was opened by the smell of incense and threatened to close when the censer was empty. Nor does one see in characters three times as large as those of the text any respectful homage to some elevated dignitary of science, to a scholar-patron, something, however, indispensable (I was about to say inevitable) for someone at the age of twenty who wants to write. I say to no one that I owe to his counsel or his encouragement everything of value in my work. I do not say it, because it would be to lie. If I have anything to say to the great men of the world or to the great men of science (and the way things are now the distinction is imperceptible) I swear that it would not be to give thanks. To some I owe the late appearance of two memoirs,

to others having to write everything in prison, a stay that one is wrong to think an occasion for reflection, and where I was often astonished at my carefree manner of shutting the mouths of my carping critics, and I am sufficiently convinced of the baseness of my critics that I think I can use the word carping without any fears for my modesty. It's not my purpose to explain how and why I was detained in prison, but I have to say how often manuscripts lose themselves among the papers of Messieurs the members of the Institute, although I have difficulty in conceiving such a casualness on the part of men who have the death of Abel on their conscience. Since I don't want to compare myself to this illustrious geometer, it's enough to say that my memoir on the theory of equations was submitted, in essence, to the Academy of Science in February 1830, that extracts of it had been sent in 1829, that no report resulted, and that it has been impossible to recover the manuscripts. There are very strange stories of this sort, but it would be graceless to recount them, because I have met no accident of this sort, except for the loss of my manuscripts. Happy traveler, my sullen mug has saved me from the jaws of the wolves. I have already said more than enough to make the reader understand that no matter how well-intentioned I may have been, it would have been absolutely impossible for me to grace or disgrace, as one likes, my work with a dedication.

Secondly, the two memoirs are short and not at all proportional to the titles; moreover they contain at least as much French as algebra, to such a point that, when the manuscripts were brought to him, the printer thought in good faith that it was an introduction. In this regard I am completely inexcusable; it would have been so easy to repeat the rudiments of the whole theory, on the pretext of having to present it in the form necessary for the comprehension of the work, or even better to present a whole branch of science larded with two or three new theorems but without indicating which were new. It would have been so easy to substitute all the letters of the alphabet in each equation, numbering them by order in order to recognize what combination of letters each of the subsequent equations referred to; which would have multiplied indefinitely the number of equations, especially if one recalls that after the Latin alphabet, there is the Greek, and this exhausted there are Gothic letters, that nothing prevents the use of Syrian characters, and if necessary even Chinese characters. It would have been so easy to transform each phrase ten times, taking care to precede each transformation with the solemn word of theorem, are even better to arrive with the help of OUR ANALYSIS at results known since the time of the good Euclid, or finally to ensure that each proposition was preceded and following by a procession of particular examples. In spite of all these means, I was not able to use a single one.

Thirdly, the first memoir was not chaste of the master's eye; an extract sent in 1831 to the Academy of Sciences was submitted for examination to M. Poisson, who admitted in one of its sessions to not having understood it at all. In my eyes, fascinated as I am by an author's vanity, this proves simply that M. Poisson was either not willing or not able to understand, but in the public's eyes will mean that my book was worth nothing.

Everything suggests to me therefore that in the learned world, the work that I am submitting to the public will be received with a compassionate grin, that the most indulgent will tax me with clumsiness, and that for some time I shall be compared to Wronski and to those indefatigable men who discover every year a new solution to the problem of squaring the circle. I shall above all have to bear the

guffaws of the examiners of candidates at the École Polytechnique (*who had failed him!*) (who, in passing, to my astonishment do not occupy each and every one a chair of the academy of science because they certainly do not belong to posterity) and who, tending to monopolize the publication of books on mathematics, will not discover without being offended that a young man, twice rejected by them has the pretension to write, not didactic texts, but theoretical texts.

I have said all this in order to prove that I am wittingly exposing myself to the ridicule of fools.

If I publish in spite of everything, with little chance of being understood, the fruits of all my late nights, it is in order to fix a date for my researches, it is in order that the friends I have made in the world know, before I am locked up, that I'm very much alive, it's perhaps also in the hope that this research could fall into the hands of people who will not be prevented from reading it by a stupid arrogance and could direct them into the new path that must, according to me, pursue analysis into its highest branches. It's necessary to be clearly aware that I am speaking here of pure analysis; my assertions if transferred to the most direct applications of mathematics would become paradoxical.

Long algebraic calculations were at first of little need to the progress of mathematics, very simple theorems gained little from being translated into the language of analysis. It's only since Euler that this briefer language has become indispensable to the new extension that this great mathematician has given to the science. After Euler, calculations have become more and more necessary, but more and more difficult to the extent that they were applied to more advanced topics of science. Since the beginning of this century, the algorithm had attained such a degree of complication that with it no progress was possible without the elegance that modern mathematicians were able to impose on their research, by means of which the mind was able to grasp promptly at one swoop a large number of operations.

It is clear that the elegance much praised, and with good reason, has this as its sole aim.

By the well-confirmed fact that the efforts of the most advanced mathematicians aim at this elegance, one can conclude with certitude that it becomes more and more necessary to embrace several operations at once, because the mind no longer has the time to attend to all details.

Now I believe that the simplifications produced by the elegance of the calculations (intellectual simplifications of course; there are no material simplifications) have their limits; I believe that the moment will arrive where the algebraic transformations foreseen by the speculations of the analysts will find neither time nor place to occur; to such a point that it will be necessary to be content with having foreseen them. I don't want to say that there is nothing more for analysis without this help, but I believe that without one day everything will be exhausted.

To take a bold leap at these calculations; to group them according to their difficulties and not according to their forms; that is, according to my view, the mission of future mathematicians; that is the path I have taken in this work.

It is necessary not to confuse the opinion expressed here with the affectation of certain persons to evade in appearance every sort of calculation, by translating by long sentences that which can be expressed very simply by algebra, thereby adding to the length of the operations the length of a language not made to express them. Those persons are a hundred years behind the times.

Here there is nothing of the sort; here the analysis is analyzed; here the most advanced calculations carried out until present are considered as particular cases, that it was necessary, even indispensable to handle, but that it would be baneful not to abandon for research on a broader scale. The time to execute the calculations foreseen by this higher analysis and classified according to their difficulty but not according to their form will arrive when a particular question requires it.

The general thesis that I am proposing will not be understood without reading this work, which is an application of it, attentively: not that the theoretical point of view preceded the application; but I asked, my book finished, what made it appear so strange to most readers, and looking inside myself, I thought I observed just such a tendency of my spirit to avoid calculations in the subjects treated and, what is more, I recognized an insurmountable difficulty that would be met by anyone wishing to carry them out generally with the matter treated.

It should be foreseen that, when treating such new domains, when risking oneself in such new paths, I have met difficulties that I could not overcome. Thus in these two memoirs and in particular in the second, which is more recent, the phrase "I do not know" appears frequently. The class of reader that I mentioned at the beginning will certainly find this an occasion for laughter. It's unfortunate that they will not suspect that the book the most valuable and the most learned is the one in which the author says everything that he does not know, that they do not suspect that an author never does more damage to his readers than when he hides a difficulty. When the reign of competitiveness, thus of vanity, in the sciences ends, when one cooperates for studying, rather than sending sealed packets to academies, one will be eager to publish the simplest observation, provided they are new, and one will add "I don't know the rest".

From Sainte-Pélagie, X, 1831

Preliminary discourse

The following memoir was sent about seven months ago to the academy of sciences in Paris, and misplaced by the commissioners who were to examine it. The work has therefore acquired no prestige that would encourage reading it; and this is not the only reason that has kept the author from publishing it. If he finally decided to do so, it is for fear that more adept mathematicians, taking over the same field, may cause him to lose entirely the fruits of a long labor.

The aim that has been proposed is to characterize equations that can be solved by radicals. We can affirm that no domain more obscure and isolated from the rest exists in pure analysis. The novelty of the material has required the usage of new terminology and of new characteristics. We have no doubt that this inconvenience will rebuff from the beginning the reader who can scarcely pardon the use of a new language even to authors for whom he has every respect. But finally, we have had no choice but to conform to the demands of the subject, whose importance merits a certain attention.

Given an equation algebraic with arbitrary coefficients, numeric or literal, determine whether the roots can be expressed by radicals, is the question to which we offer a complete solution.

If now, you give me an equation that you have in any way you like and if you want to know whether it is or not solvable by radicals, I have nothing to do but to

indicate to you the way to reply to the question, but without obliging either myself or anyone else to do so. In a word, the calculations are impracticable.

Accordingly, it appears that there are no fruits to harvest from the solution that we propose.

Indeed it would be so if the question presented itself ordinarily from this point of view. But most times, in applications of Algebraic Analysis, one is led to equations whose properties one knows in advance: properties by means of which it will always be easy to reply to the question by the rules we propose. There exists in effect for these kinds of questions a certain order of metaphysical consideration that float over all the calculations and often render them unnecessary. I cite for example the equations that give the division of elliptic curves and that the celebrated Abel solved. It is certainly not because of their numerical form that this mathematician succeeded. What makes the theory beautiful and at the same time difficult is that unceasingly one indicates the progress of the calculations and foresees their result without ever being able to effect them. I cite as well the modular equations,

Observe that the discourse ends with a comma!

Historical background for Kummer from German History 1770–1866 by J. J. Sheehan

It can begin with the Revolution of 1848, which in France led to the fall of Louis-Philippe and a brief victory for the republicans. I quote some passages from Sheehan's book.

> ..., on 22 February, the streets of Paris were filled with anti-government demonstrators; the next day they built barricades and fought with royal troops; on the day after that King Louis Philippe fled.

The revolution spread.

> Beginning in the south-west at the end of February, a wave of unrest spread through the German states until it reached the Russian frontier. In hundreds of cities, towns, and villages, people demanded political reform, social justice, and relief from misery and servitude... With the possible exception of the months immediately after the First World War, there is no other period in German history so full of spontaneous social action and dramatic political possibilities.

March 13. Metternich, the Austrian chancellor, resigns after protests, demonstrations and violence in Vienna.

> Metternich wrote a brief letter relinquishing all his posts; twenty-four hours later, in disguise and with money borrowed from the Rothschilds, he left the city to begin a long and circuitous passage to England, where he joined other casualties of the revolution such as Louis Philippe, Guizot, Prince William of Prussia, and Lola Montez.

In Austria,

> Moderate opinion was delighted by the emperor's proclamation of 15 March which abolished censorship, ..., and promised to convene a constitutional assembly ... But in order to enjoy these

> newly won achievements, it would be necessary to have peace and domestic tranquility. The violence, which the moderates had used for their own end on 13 March, had to stop. Count Hoyos, the new commander of the Civil Guard, called upon responsible people to join his fight against 'the wild, criminal impulses of the proletariat'.

So we see a conflict between liberal and proletarian elements that will be reflected in Kummer's letter to Kronecker. In Prussia, whose king Friedrich Wilhelm the fourth was later to be declared mentally incompetent, so that his responsibilities were assumed by his brother as regent, and especially in Berlin, the same forces were at work.

> Finally, on the evening of 17 March, Frederick William approved plans that met some of the moderates' most important demands ... On the morning of the 18th, however, the king appointed General von Prittwitz, a hard-liner, as military commander of Berlin. Prittwitz's troops, apparently frightened by the presence of a large and peaceful gathering in front of the royal palace, fired into the crowd, killing several civilians. People reacted furiously ... We do not know the social position of those who fought against the king's soldiers, but we do know the identities of many who died in the fighting. Most of them were males ... between the ages of twenty and thirty-five; they included a few members of the *Bärgertum* ... and some manual workers, but the overwhelming majority consisted of craftsmen.
>
> The bloody events of 18 March made a shambles out of Frederick William's attempt to channel the opposition into a moderate course. That evening he faced in stark and unyielding terms what he had been trying to avoid for a fortnight—the choice between determined resistance or unambiguous surrender to popular demands ... Early in the morning of 19 march, he wrote his famous proclamation 'An meine lieben Berliner!' which accepted the insurgents' key demand ... Theodor Fontane, who had spent the evening crouched on a barricade in Alexanderplatz (*he was an apprentice in a pharmacy a few hundred yards away*) recalled the feelings of joy and exaltation with which he and his comrades learned of the king's decision. Victory was theirs—but ... the revolution's triumph had been given them as a gift and could just as easily be taken back.

Fontane describes his experiences on March 18 in his Autobiography, from which I shall take his description of the elections.

Somewhat earlier, the diet in Frankfurt, the seat of the Confederation of German states had begun to respond to events.

> Finally, on March 10, a majority of the diet's membership—some acting without instruction from their governments—called upon the various German states to send 'men trusted by the public' to Frankfurt in order to draft a new federal constitution.
>
> The so-called *Vorparlament*, (*basically a self-selected group*) ... met in Frankfurt on 31 March ... (it) voted in favor of elections

> for a constituent assembly and established a committee of fifty to help administer them.

Preparations for the elections begin.

> With few exceptions ... the states established a two-step ballot while the *Vorparlament* specifically outlawed limiting the franchise on religious or financial grounds, it did say that only 'mature, independent' citizens (and this meant *male* citizens) could vote or be elected to office ... In some states, however, the authorities used this term to exclude the lower orders.

The newly elected parliament first met on May 18. The events described by Fontane in his Autobiography and by Kummer in his letter to Kronecker took place in the intervening weeks.

From Fontane's autobiography

In the Wool Staple—First and Last Appearance as a Politician.

> I no longer know how many weeks later the elections to a 'constituting assembly' began. A representation of the people was to be called up and the Constitution was to be confirmed by it. As is well known things turned out a lot differently, and the final result after refusal to grant taxes and dissolution of the assembly was a 'conceded constitution' and not one dictated by the will of the people.
>
> Anyhow elections to the constituting assembly. The method of election corresponded to the three-class system that had exercised its blessing up to that time and what it came to was not direct elections but indirect, in other words that an intermediary pushed himself in. This intermediary was the 'Wahlmann' (*elector*). He was generated by the Urwähler (*primary elector*) and then, in his turn, generated the deputy proper.
>
> All the details of the procedure have of course long vanished from my memory, and I still know only that I myself was old enough to make an appearance as Urwähler. I acquired therefore, I suppose, the necessary document and, equipped with it, betook myself to the premises, in which the primary electors of the Neue Königstraße and vicinity were to come to a conclusion about their Wahlmann and to grant him their political procuration. Although I say premises, this is not quite correct. According to Berlin notions premises are spots where there are many waiters lounging about who occasionally bring you a pint, even before it has been ordered. Our election premises were by no means of this sort. It was rather a large, long shed on both of whose sides enormous sacks of wool were piled high, while two of these sacks were shoved at right-angles to each other and formed a compartment, a kind of business room. In front of them a small table had been placed at which an electoral official, or someone of the sort, sat, a dignified elderly gentleman, apparently also the most intelligent, who was to take charge of events. The number of

those present was not large, at most some thirty, and as nobody quite knew what was to be done, we all stood around in groups and waited for someone, who had at least some notion of how to proceed, took matters in hand. Naive folk always have great need for direction. The electoral official finally asked if one of those who had shown up wouldn't like to suggest a possible Wahlmann. Everyone expressed agreement, but otherwise remained silent, and eyes were all turned to a lanky middle-aged gentleman, who in that excitement that is the certain sign of someone with a great urge to speak and an accompanying inability to do so paced back and forth in front of the two wool sacks. It was as much an image of misery as of comedy, accented by his dress. Whereas the rest of us, mostly small artisans, small shopkeepers or waiters, had turned up in our everyday clothes, the excited fellow wore a black frock coat and a white candidates' band. He constantly took off his glasses and put them on again and was annoyed when the stems were snagged in his wiry blonde hair.

"Who is the gentleman", I asked my neighbor.

"That's the principal of the school just across the way".

"What's his name then?"

"Schaefer I think; but it could also be Scheffer. I'll just ask Roesike ... Hey there, Roesike".

And it was apparent that for my sake he was about to cry out to his friend the baker Roesike about "Schaefer or Scheffer". He didn't get to it, as in just that moment the principal placed himself beside the table of the elderly gentleman who was directing the proceedings and said—a couple of key words remain in my mind—more or less the following "Ja, meine Herren, what has brought us together—we are gathered together here in this wide space, and each of us is certainly imbued by it. And everyone is doubtless grateful to God that we have a race of princes like ours. There is no land with such a race and we stand with it in love and loyalty ... but, my dear gentlemen, neither horse nor rider ... you know, that in this place too, there have been heroic struggles, the blood of citizens has been spilt, and victory has been on our side. We have now to chain this victory to our flag. For that we need the right men, who are aware at all times that the German spirit is incapable of baseness. And betrayal of our holiest possessions is baseness. I know that there is no one under us. But not everyone thinks and feels this way. There are still many who desire life before freedom. They tear at it with the beaks of vultures. Therefore I'm for annexation to France and I see a danger for Prussia from that man who put Poland in a coffin and who is opposed to our young freedom. Thus, meine Herren, men of proven loyalty to the king, of proven loyalty to the people: Jahn, Arndt, Boyen, Grolmann, perhaps also Pfuel. They will hold our flag high. I vote for Humboldt".

> The speech was met with applause and only the chairman smiled. But he did not feel the need to refute it, and so it fell to my wretched self, to catch the reins of the principal as he raced off in a wild chase of the most elevated goals. Much against my inclinations. I was righteously indignant over these desolate, pompous gimcrack notions, and observed accordingly that it was not given to us, here below, to concern ourselves directly with the Hohenzollerns or with freedom, but that we had no more to do here on God's earth than, in our capacity as Urwähler, to elect a modest Wahlmann. Everything else came later, then would come the time to steer Prussia to the left or to the right. I had therefore to decline on this occasion to give Alexander von Humboldt my vote, and was rather in favor of my neighbor, the baker Roesike, of whom I knew that he was a generally respected man and had the best rolls in the whole neighborhood.
>
> Since as it happened, there was no other baker present, my proposal was generally approved, but Roesike himself, free of all ambition, wanted to hear nothing about being elected, proposed rather, in considerate revenge, my name, and as, ten minutes later, we left the electoral premises, I was indeed *Wahlmann*.
>
> This was my debut in the wool staple, and at the same time my first and last appearance as a politician.

A few lines further on, he continues,

> On the evening of the same day I went out to Bethanien in order to visit Pastor Schultz ... from a few words that had just been uttered as I entered I made out with no difficulty that they were speaking of the elections and making fun of them. Schultz, otherwise a very serious man—too serious—was the heartiest of all and as he saw me making my bows from the door to the gentlemen present he called to me in a high spirits, 'What brings you here, now that you've become an elector?'
>
> I nodded.
>
> "Of course, you look exactly like one".
>
> Everybody laughed and I thought it wisest to join in, even though my insides boiling, I was saying vainly to myself, "Dear Schultz, I'll get even with you".

Fontane's mocking tone can be compared with the still amused but less distant tone of Kummer in a letter to Kronecker. At that time, Breslau had been for about one hundred years a part of Prussia, so that we can assume the electoral regulations were the same. On the other hand, Kummer's response was immediate, not written 4 and 1/2 decades after the event.

Kummer to Kronecker—Breslau, May 5, 1848

> Can you imagine, that in the last eight days I've twice tried my hand at speech-making. First of all before a meeting of our electoral district, where I spoke about the qualities of a good elector, and was very well received, and was unanimously elected chairman of the next meeting. During the first meeting I had

> reconnoitred the terrain and discovered that the democratic club prevailed through the presence of insignificant individuals, who were trying to push themselves forward as electors. In order to succeed, they flattered the workers, threw suspicion on civil servants, and availed themselves of all the usual tricks. I decided thereupon to eliminate, in my own person, at least one of these fellows and delivered a second speech directed principally at the workers. Although I applied means exactly opposite to those of the democrats, namely to point out to the workers exactly what they had achieved since the 18th March, and to imbue them with confidence in the present regime, I succeeded completely. The democrats held indeed another meeting on Sunday, where they attempted to eliminate me, but that didn't work, as you saw from the list of electors. Besides me, of course, apart from two local citizens, only members of the democratic club were elected for Frankfurt and Berlin; in fact, the democrats here won solidly. I myself am not prejudiced against the democrats. Provided that their views about the solid establishment of a thoroughly free constitutional monarchy are sincerely meant, and they don't take to the field against royalty, or attempt secretly to undermine it, I'm basically fonder of the democrats than of the philistine citizens, who hardly participate any longer in the elections for Frankfurt, because they have little if any interest in them. The demands that I place on a deputy to Berlin are 1) true love of the fatherland, 2) insight and understanding, 3) strength of character. I place no special demands, because after all we have to take the candidates that are left after the narrower and narrowest choices. We'll be lucky if we, in the end, can choose from two good candidates the best. It's certainly possible that in the end we'll have to choose the lesser of two evils. For a deputy to Frankfurt the demands would be the same, but the love of the fatherland would have its roots more in a single Germany than in Prussia, and the insight extend more to the general.—I am very proud of my title of elector, as you can see from the circumstance that in Fürstenstein, where we were on Wednesday, I registered myself as E. Kummer, *Wahlmann*, my wife as *Wahlweib*, my cousin as *Urwähler* and Louise Cauer as *Wahlverwandtschaft*.

We have already met several Urwähler. I recall that *Wahlverwandtschaft* means *elective affinity*; so this is an allusion either to Goethe or to a now outmoded chemical doctrine. (rpl)

> I am really pleased with my success, in particular because my sincere patriotism allowed me to overcome my timidity and to stand up and speak before such a mixed assembly. As soon as I have done my duty as a citizen, namely immediately after the elections for the Frankfurt assembly, I shall return with all my forces to my mathematical work, as I'll have for the moment nothing more political to do. If you visit me next week, as I am hoping, then I'll recount more about the local elections and

> give you the draft of my first speech. The second was almost spontaneous, and only vaguely planned. All the best ... and the best of greetings from all my family.

In order to see what Kummer met when he as Wahlmann elected the deputy, I continue with Fontane's account.

Sequel—Berlin in May and June, 1948.

> I have spoken earlier of my status as elector and the oratorical achievements in the wool staple in the Neue Königstraße leading to it as my 'first and last appearance as politician'. I should add that this 'first and last appearance as politician' had as one of its components a sequel. The sequel was the assembly of Wahlmänner for the purpose of the election of a deputy. I was elected in wool staple in the Neue Königstraße. I was to elect, or at least to take part in the deliberations, in the concert hall of the Royal Theatre. That I did, and I count the hours in which the deliberations took place among my happiest. Everything was full of life and interest, even though in respect of genuine politics every modern politician would turn his face in disgust. Things were said precisely of the best men that had almost no relation to the subject to be treated there; but so bizarre, often even bordering on the comic, these shots in the treetops appeared, there was still something in the expectorations of these dilettantes. The old General Reyher—Chief of the General Staff and the predecessor of Moltke, who often spoke gratefully of him as his teacher—spoke once, and briefly offered a confession of faith, perfectly useless in connection with the matters that we were there to settle. It made, nevertheless, a great impression on me to hear a distinguished old general confess freely to his faith in his king and in the army, for one heard then very little of such things. And then, on the same day I believe, the old *Jakob Grimm* stepped up to the podium, the wonderful head—fixing itself in the memory like the head of Mommsen, in a halo of long snow-white hair, and spoke something completely general about Germany, that in any proper political gathering would have brought shouts of 'to the point' down on his head. This shout was, however, not heard because everyone was moved by the sight and felt, that no matter how far away all of that might lie, it was to be followed, willy-nilly.
>
> Those were two splendid figures that remained in my memory forever, while the others were by and large chatterboxes and nullities, a few even confidence men.

Kummer would have enjoyed such a gathering! In general, Kummer, in contrast to Galois, seems to have been neither rebellious nor dissatisfied. He took life and the world about him as it came with considerable good humor. He was a one-year volunteer in the Prussia army as a young man, enjoyed a hunting party, and was fairly gregarious. He also seems, and that is unusual for a mathematician of his caliber, to have been a competent and respected administrator. He became rector

at Breslau on October 15, 1848. The university at Breslau (the present Wrocław) was presumably not very large, and his responsibilities not overwhelming, but in the aftermath of the March revolution he undoubtedly had to steer an uneasy course between the students and the Prussian university administration. The speech he gave on assuming the office of rector is extant. It is a lecture on academic freedom and the purpose of the university. It is long and I do not cite it at length. Besides, to understand it would require more understanding of the details of the university reforms than I possess. I am not certain what Kummer is defending as academic freedom. It would not be uninteresting to examine the full speech with more care. I content myself with quoting two passages.

One from the beginning

> On the assumption of the rectorate of the university, now in a time in which our entire fatherland has made progress that is of the highest significance in its historic development and that has set in great motion all members and institutions of the state, and therefore our university as well, I am seized by a certain uneasiness, for I do not know how far I shall succeed in fulfilling the high duties that this office imposes on me. The academic year, that now lies ahead of us, will acquire no doubt, just as the year now ending, more than usual significance through the numerous improvements and new arrangements that it will call into being, which satisfy the needs of the present and the generally awakened freer spirit. The more important and the more pregnant with consequences this progress is, the heavier is the responsibility that I assume as Rector, but the greater is the urge in me to devote myself with the entire force of my being to the care of the prosperity and well-being of the University. Indeed, in the firm hope that the newly awakened political life in our Fatherland, even with all the contending contradictions with which it is imbued, will further the well-being of our institution, my unease vanishes, and I am delighted that it is now granted to me to participate fervently in this progress.
>
> The German universities, as the highest institutions of learning of our fatherland, as the hearths of the spirit of our nation, have from the beginning not only incorporated this spirit but also developed and propagated it through teaching and writing. They have thereby not alone moved ahead with the times, but in so far as the true progress of the spirit has been nursed at their bosom, they have even outpaced the times. To mention only one thing, one of the grandest blossoms of the present, the idea of German unity has been for more than thirty years cultivated almost solely by the universities, at a time, when it went almost unnoticed by the people and when the governments attempted to suppress and extirpate it with various measures and punishments.

One from the middle

> I want therefore to limit myself here to mentioning one of the significant rights that were won for the entire German nation through the overthrow of the old administrative system, the right of association, which is of great importance for the universities too, specifically for the forms of academic freedom in the life of students. There is no doubt, that this right is also available to the students, and that the expected new academic laws in no way restrict it, but that rather only certain forms are to be respected by the student associations, if they are going to be recognized as such by the university authorities.

Further Dates

1864–1666: Forcible consolidation of Prussia's position at the expense of Austria.
1870–1871: Franco-Prussian war, creation of the German empire.

As secretary of the Royal Prussian Academy of Science, Kummer was called upon to give speeches on various occasions, anniversaries of Friedrich the second and of Leibniz, or anniversaries of the reigning king Wilhelm the First. Sometimes he takes the occasion to comment on mathematical developments, such as the importance of the contributions of Jacobi and Dirichlet in the development of a real school in Berlin or to relate somewhat anodyne histories of the development of mathematical ideas. He has a taste for history and was, for better or worse, carried away to some extent by the increasingly chauvinistic and militaristic temper of the times. There is a good deal to be learned from the response of a sympathetic figure, like Kummer, to historic changes that most of us find, in retrospect, distressing. The 1877 speech on the occasion of the birthday of Wilhelm the First, who was born in 1797, died in 1888, and who became King of Prussia in 1861 and the German emperor in 1871, is an account of Wilhelm's military career, which began at the age of nine, and is informed by the then prevailing enthusiasm for the military. Kummer, like Dirichlet, supplemented his income with a position at the Military Academy, so that he would have had occasion to inform himself of military matters. The speech appears, although I have not yet read it in full, to make for good and instructive reading. I have as yet only glanced at the others.

I

DEUX MÉMOIRES D'ANALYSE PURE PAR [E. GALOIS]

PRÉFACE

Cecy est un livre de bonne foy.
MONTAGNE.

72 a Premièrement, le second feuillet de cet ouvrage n'est pas encombré par les noms, prénoms, qualités, dignités et éloges de quelque prince avare dont la bourse se serait ouverte à la fumée de l'encens avec menace de se refermer quand l'encensoir serait vide. * On n'y voit pas non plus, ⌜en caractères trois fois gros comme le texte⌝, un hommage respectueux à * quelque haute position dans les sciences, à un savant protecteur, chose pourtant indispensable (j'allais dire inévitable) * pour quiconque ⌜à vingt ans * veut écrire⌝. Je ne dis à personne que je doive à ses conseils ou à ses encouragements tout ce qu'il y a de bon dans mon ouvrage. Je ne le dis pas : car ce serait mentir. Si j'avais à adr *esser q-* uel *que* chose aux grands du monde ou aux grands de la science (et au temps qui court la distinction est imperceptible entre ces deux classes de personnes), je jure que ce ne seraient point des remerciements. * Je dois aux uns de faire paraître si tard le premier des deux mémoires, aux autres d'avoir écrit le tout en prison, séjour que l'on a tort de considérer comme un lieu de recueillement, et où je me suis souvent trouvé stupéfait de mon insouciance à fermer la bouche à mes stupides Zoïles : * et je crois pouvoir me servir de ce mot de Zoïle en toute sûreté pour ma modestie, tant * mes adversaires sont bas dans mon

esprit. * Il n'est pas de mon sujet *de dire* comment et pourquoi l'on me retient en prison ** : mais je dois dire comment les manuscrits s'égarent le plus souvent dans les cartons de MM. les membres de l'Institut * quoiqu'en vérité je ne conçoive pas une pareille insouciance de la part des hommes qui ont sur la conscience la mort d'Abel. ⌜A moi qui ne veux pas me comparer à cet illustre géomètre⌝, il suffira de dire que mon mémoire sur la théorie des équations a été déposé ⌜en substance⌝ à l'académie des sciences au mois de février 1830, que des extraits en avaient été envoyés en 1829, qu'aucun rapport ne s'en est suivi et qu'il m'a été impossible de revoir les manuscrits. Il y a dans ce genre des anecdotes fort curieuses * : mais j'aurais mauvaise grâce à les * raconter, parce qu'aucun accident ⌜semblable⌝, sauf la perte de mes manuscrits, ne m'est arrivé. Heureux voyageur, ma mauvaise mine m'a sauvé de la gueule des loups. J'en ⌜ai⌝ déjà trop dit pour faire comprendre au lecteur pourquoi, * quelle que fût d'ailleurs ma bonne volonté, il m'eût été absolument impossible de * parer ou de déparer, comme on voudra mon œuvre d'une dédicace.

72 b En second lieu, les deux mémoires sont courts et nullement proportionnés aux titres *; et puis il y a au moins autant de français que d'algèbre à tel point que l'imprimeur, quand on lui a porté les manuscrits, a cru de bonne foi que c'était * une introduction. En ce point je suis ⌜complètement⌝ inexcusable; il eût été si facile de reprendre dans ses éléments toute une théorie, sous le prétexte de la présenter sous une forme nécessaire à l'intelligence de l'ouvrage, ou bien mieux sans plus de façon * d'entrelarder une branche de science de deux ou trois théorèmes nouveaux, sans désigner lesquels ! * Il eût été si facile encore de substituer successivement toutes les lettres de l'alphabet dans chaque équation, en ⌜les⌝ numérotant par ordre * pour pouvoir reconnaître * à quelle combinaison de lettres appartiennent les équations subséquentes; ce qui eût multiplié indéfiniment le nombre des * équations, si l'on réfléchit qu'après l'alphabet latin, il y a encore l'alphabet grec, que, celui-ci é *puisé* , il reste les caractères allemands, que rien n'empêche de se servir des lettres syriaques, et au besoin des lettres chinoises ! Il eût été si facile de transformer dix fois chaque phrase, en ayant soin de faire précéder chaque transformation du mot solennel théorème; ou bien encore d'arriver par

NOTRE ANALYSE à des résultats connus depuis le bon Euclide; ou enfin de * faire précéder et suivre chaque proposition d'un cortège redoutable d'exemples particuliers ! Et de tant de moyens je n'ai pas su choisir un seul !

En troisième lieu, le premier mémoire n'est pas * vierge de l'œil du maître; un extrait envoyé en 1831 ⌜à l'académie des sciences⌝, * a été soumis à l'inspection de M. Poisson, qui est venu dire ⌜en séance⌝ ne point l'avoir compris. Ce qui, * à mes yeux fascinés par l'amour-propre d'auteur, prouve simplement que M. Poisson n'a pas voulu ou n'a pas pu comprendre, mais prouvera certainement aux yeux du public que mon * livre ne signifie rien.

[Tout concourt donc à me faire penser que dans le monde savant, * l'ouvrage que je soumets au public sera reçu avec le sourire de la compassion; ⌜que * les plus indulgents me taxeront de maladresse⌝; et que pendant quelque temps je serai comparé à Wronski ou à ces hommes * infatigables qui trouvent tous les ans une solution nouvelle de la quadrature du cercle. J'aurai surtout à supporter le rire * fou de MM. les examinateurs des **73 a** candidats à l'École Polytechnique, (que je m'étonne ⌜en passant⌝ de ne pas voir occuper ⌜chacun⌝ un fauteuil à l'académie des sciences, car leur place n'est certainement pas dans la postérité) * ⌜et qui ayant tendance à monopoliser l'impression des livres de mathématiques n'apprendront pas sans en être formalisés⌝ qu'un jeune homme deux fois mis au rebut par eux a aussi la prétention * d'écrire, non des livres didactiques ⌜il est vrai⌝, mais des livres de doctrine. *

* Tout ce qui précède, je l'ai dit pour prouver que c'est sciemment que je m'expose à la risée des sots.]

Si avec aussi peu de chances d'être compris, je publie, malgré tout, le fruit de mes veilles, c'est * afin de prendre date pour mes recherches, c'est afin que les amis que j'ai formés dans le monde avant qu'on m'enterrât sous les verrous, sachent que je suis bien en vie, ** c'est peut-être ⌜aussi⌝ dans l'espérance que ces recherches * pourront tomber entre les mains de personnes à qui une morgue ⌜stupide⌝ * n'en interdira pas la lecture, * et les diriger dans la nouvelle voie que doit, selon moi, suivre l'analyse dans ses branches les plus hautes. Il faut bien savoir que je ne parle ici que d'analyse pure; mes assertions transportées aux applications les plus directes des mathématiques deviendraient paradoxales.

Les ⌜longs⌝ calculs algébriques ont d'abord été * peu nécessaires au progrès des Mathématiques, les théorèmes fort simples gagnaient à peine à être traduits dans la langue de l'analyse. Ce n'est ⌜guère⌝ que depuis Euler que * cette langue plus brève est devenue indispensable à la nouvelle extension * que ce grand géomètre a donnée à la science. * Depuis Euler les calculs sont devenus ⌜de plus en plus nécessaires, mais⌝ de plus en plus * difficiles ⌜à mesure qu'ils s'appliquaient à des objets de science plus avancés⌝. Dès le commencement de ce siècle, l'algorithme avait atteint un degré de complication tel que tout progrès était devenu impossible par ce moyen, sans l'élégance que les * géomètres modernes ont su imprimer à leurs recherches, et * au moyen de laquelle l'esprit saisit promptement et d'un seul coup un grand nombre d'opérations.

Il est évident que l'élégance si vantée et à si juste titre, n'a pas d'autre but.

Du fait bien constaté que les efforts des géomètres les plus avancés ont pour objet l'élégance, * on peut donc * conclure avec certitude qu'il devient de plus en plus nécessaire d'embrasser plusieurs opérations à la fois, parce que l'esprit n'a plus le temps de s'arrêter aux détails.

Or je crois que les simplifications produites par l'élégance des calculs, (simplifications intellectuelles, s'entend; de matérielles il n'y en a pas) ont leurs limites; je crois que le moment * arrivera **73 b** où les transformations algébriques prévues par les spéculations des analystes ne trouveront plus ni le temps ni la place de se produire; à tel point qu'il faudra se contenter de les avoir prévues. * Je ne veux pas dire qu'il n'y a plus rien de nouveau pour l'analyse sans ce secours : mais je crois qu'un jour sans cela tout serait épuisé.

* Sauter à pieds joints sur ces calculs; * grouper les opérations, les * classer suivant leurs difficultés et non suivant leurs formes; telle est, suivant moi, la mission des géomètres futurs; telle est la voie ou je suis entré dans cet ouvrage.

Il ne faut pas confondre l'opinion que j'émets ici, avec l'affectation que certaines personnes ont d'éviter ⌜en apparence⌝ toute espèce de calcul, ⌜en⌝ traduisant par des phrases fort longues ce qui s'exprime très brièvement par l'algèbre, et ajoutant ainsi à la longueur * des opérations, les longueurs d'un langage qui

n'est pas fait pour * les exprimer. Ces personnes-là sont en arrière de cent ans.

Ici rien de semblable; ici on fait l'analyse de l'analyse : ici les calculs * les plus élevés ** exécutés jusqu'à présent sont considérés comme des cas particuliers, qu'il a été utile, indispensable de traiter, mais qu'il serait funeste de ne pas abandonner pour des * recherches plus larges. Il sera * temps d'effectuer des calculs prévus par cette haute analyse et classés suivant leurs difficultés, mais non spécifiés dans leur forme, quand * la spécialité d'une question les réclamera.

La thèse ⌜générale⌝ que j'avance ne pourra être bien comprise que * quand on lira attentivement mon ouvrage qui en est une application : non que * ce point de vue théorique ait précédé l'application; mais je me suis demandé, mon livre terminé, ce qui le rendrait si étrange à la plupart des lecteurs, et * rentrant en moi-même, j'ai cru observer cette tendance de mon esprit à éviter * les calculs ⌜dans les sujets que je traitais⌝, et qui plus est, ⌜j'ai reconnu⌝ une difficulté insurmontable à qui voudrait les effectuer ⌜généralement⌝ dans les matières que j'ai traitées.

* On doit prévoir que, traitant des sujets aussi nouveaux, hasardé dans une voie aussi insolite, bien souvent des difficultés se sont présentées que je n'ai pu vaincre. Aussi dans ces deux mémoires et surtout dans le second qui est plus récent, trouvera-t-on souvent la formule « je ne sais pas ». La classe des lecteurs dont j'ai parlé au commencement ne manquera pas d'y trouver à rire. C'est que malheureusement on ne se doute pas que le livre le plus précieux du plus savant serait celui où il * dirait tout ce qu'il ne sait pas, ⌜c'est qu'on ne se doute pas⌝ qu'un auteur ne n*uit* jamais tant à ses lecteurs que quand il dissimule une difficulté. Quand ⌜la concurrence c'est-à-dire⌝ l'égoïsme ne règnera plus dans les sciences, quand on s'associera pour étudier, * au lieu d'envoyer aux académies des paquets cachetés, on s'empressera de publier ses moindres observations pour peu qu'elles soient nouvelles, et on ajoutera : « je ne sais pas le reste ».

De Ste Pélagie Xbre 1831,

EVARISTE GALOIS.

I

DISCOURS PRÉLIMINAIRE

59 a Le mémoire qui suit a été * adressé il y a * environ sept mois à l'académie des sciences de Paris, et égaré par les commissaires qui devaient l'examiner. Cet ouvrage * n'a donc, pour se faire lire, acquis aucune autorité :, et cette raison n'était pas la dernière qui retenait l'auteur dans sa publication. S'il s'y décide, c'est par crainte que des géomètres plus habiles, en s'emparant du même * champ, ne lui fassent perdre ⌜entièrement⌝ les fruits d'un long travail.

* Le but que l'on s'est proposé est de déterminer des caractères pour la résolubilité des équations par radicaux. * Nous pouvons affirmer qu'il n'existe pas dans l'Analyse pure de matière plus obscure et peut-être plus isolée * de tout le reste. La nouveauté * de cette matière a exigé l'emploi de nouvelles dénominations, de nouveaux caractères. Nous ne doutons pas que cet inconvénient ne rebute dès les premiers pas le lecteur qui pardonne à peine aux auteurs ⌜mêmes⌝ qui ont tout son crédit, de lui parler un nouveau langage. Mais enfin, force nous a été de nous conformer à la nécessité du sujet, * dont l'importance mérite sans doute quelque attention.

* Étant donnée une équation algébrique à coefficients quelconques, numériques ou littéraux, * reconnaître si les racines **59 b** ne peuvent s'exprimer * en radicaux, telle est la question dont nous offrons une solution complète.

Si maintenant vous * me donnez une équation que vous aurez choisie à votre gré, ⌜et que vous désiriez connaître si elle est ou non resoluble par radicaux⌝, je n'aurai rien à y faire que de vous indiquer le moyen * de répondre à votre question, sans vouloir charger ni moi ni personne de le faire. En un mot les calculs sont impraticables.

* Il paraîtrait d'après cela qu'il n'y a aucun fruit à tirer de la solution que nous proposons *.

[En effet] il en serait ainsi si la question se présentait ordinairement sous ce point de vue. Mais, la plupart du temps, dans les applications de l'Analyse Algébrique, on est conduit à des équations dont on connaît d'avance toutes les propriétés : propriétés au moyen desquelles il sera toujours aisé de répondre à la question * par les règles que nous exposerons. Il existe en effet pour ces sortes de questions un certain ordre de * considérations Métaphysiques qui planent sur tous les calculs, et qui souvent les rendent inutiles. Je citerai par exemple les équations qui donnent la division des fonctions Elliptiques, et que le célèbre Abel a résolues *. Ce n'est certainement pas d'après leur forme numérique que ce géomètre y est parvenu. * Tout ce qui fait la beauté et à la fois * la difficulté de cette théorie, c'est qu'on a [sans] cesse à indiquer la marche * de l'analyse et à en prévoir les résultats sans jamais pouvoir les effectuer. Je citerai encore les équations modulaires, *

DER ACHTZEHNTE MÄRZ

VIERTES KAPITEL

Auf dem Wollboden — Erstes und letztes Auftreten als Politiker

Ich weiß nicht mehr, um wieviel Wochen später die Wahlen zu einer Art »Konstituante« begannen. Eine Volksvertretung sollte berufen und durch diese dann die »*Verfassung*« festgestellt werden. Bekanntlich kam es aber erheblich anders, und das Endresultat, nach Steuerverweigerung und Auflösung der Versammlung, war *nicht* eine vom Volkswillen diktierte, sondern eine »oktroyierte Verfassung«. Es ist immer mißlich, wenn die Freiheitsdinge mit etwas Oktroyiertem anfangen.

Also Wahlen zur Konstituante! Der dabei stattfindende Wahlmodus entsprach dem bis diesen Augenblick noch seine sogenannten Segnungen ausübenden Dreiklassensystem und lief darauf hinaus, daß nicht direkt, sondern indirekt gewählt wurde, mit anderen Worten, daß sich eine Zwischenperson einschob. Diese Zwischenperson war der »Wahlmann«. Er ging aus der Hand des Urwählers hervor, um dann aus seiner – des Wahlmanns – Hand wiederum den eigentlichen Volksvertreter hervorgehen zu lassen.

Alle Detailbestimmungen sind meinem Gedächtnisse natürlich längst entfallen, und ich weiß nur noch, daß ich persönlich alt genug war, um als »Urwähler« auftreten zu können. Ich erhielt also mutmaßlich den entsprechenden Zettel und begab mich, mit diesem ausgerüstet, in ein Lokal, in welchem sich die Urwähler der Neuen Königstraße samt Umgegend über ihren »Wahlmann« schlüssig machen und diesen ihren politischen Vertrauensmann proklamieren sollten. Wenn ich eben sagte: »in ein Lokal«, so ist dies nicht ganz richtig. Ein »Lokal« ist nach Berliner Vorstellung eine Örtlichkeit, drin viele Kellner umherstehen und einem unter Umständen ein Seidel bringen, noch ehe man es bestellt hat. Ein solches »Lokal« war nun aber unser *Wahl*lokal keineswegs; es war vielmehr ein großer, langer Boden, an dessen Seiten mächtige Wollsäcke hochaufgetürmt lagen, während zwei dieser Säcke sich im rechten Winkel quer vor-

schoben und einen Abteil, eine Art Geschäftsraum herstellten. In Front davon war ein Tischchen aufgestellt, an dem ein Wahlkommissar oder etwas dem Ähnliches saß, ein würdiger alter Herr, auch ganz augenscheinlich der klügste, der den Gang der Ereignisse zu leiten hatte. Die Zahl derer, die sich eingefunden, war nicht groß, höchstens einige dreißig, und weil wohl niemand recht wußte, was zu tun sei, stand man in Gruppen umher und wartete, daß irgendwer, der wenigstens einen Schimmer habe, die Sache in die Hand nehmen würde. Naive Menschen sind immer sehr führungsbedürftig. Endlich fragte der Wahlbeamte, ob nicht einer der Erschienenen Vorschläge hinsichtlich eines aufzustellenden Wahlmannes machen wolle. Man drückte Zustimmung aus, blieb aber schweigsam und sah nur immer zu einem langen Herrn von mittleren Jahren hinüber, der in jener Erregung, die das sichere Kennzeichen eines starke Redelust mit Redeunvermögen vereinigenden Menschen ist, in Front der beiden Wollsäcke auf und ab schritt. Er war ebensosehr ein Bild des Jammers wie der Komik, wozu seine Kleidung redlich beisteuerte. Während wir andern alle, meist kleine Handwerker, Budiker und Kellerleute, in unsrem Alltagsrock erschienen waren, trug der aufgeregte Mann einen schwarzen Frack und eine weiße Kandidatenbinde. Die Brille nahm er beständig ab und setzte sie wieder auf und war ärgerlich, wenn sich die beiden Häkchen in seinem angekräuselten blonden Haar verfitzten.

»Wer ist der Herr?« fragte ich einen neben mir Stehenden.

»Das ist der Herr Schulvorsteher von hier drüben.«

»Wie heißt er denn?«

»Ich glaube Schaefer; er kann aber auch Scheffer heißen. Ich werde mal Roesike fragen . . . Sage mal, Roesike . . .«

Und es war ersichtlich, daß er, mir zuliebe, seinen Freund, den Bäcker Roesike, wegen »Schaefer oder Scheffer« interpellieren wollte. Kam aber nicht dazu. Denn in ebendiesem Augenblicke hatte sich der Schulvorsteher neben dem Tisch des den Wahlakt leitenden alten Herrn aufgestellt und sagte – ein paar Schlagwörter sind mir im Gedächtnis geblieben – ungefähr das Folgende:

DER ACHTZEHNTE MÄRZ

»Ja, meine Herren, was uns hergeführt hat ... wir sind hier in diesem weiten Raum versammelt, und es ist wohl jeder von uns davon durchdrungen. Und jeder dankt auch wohl Gott, daß wir ein Fürstengeschlecht haben wie das unsrige. Kein Land, das ein solches Geschlecht hat, und wir stehen zu ihm in Liebe und in Treue ... Aber, meine Herren, nicht Roß, nicht Reisige ... Sie wissen, auch an dieser Stelle ist heldenmütig gekämpft worden, Bürgerblut ist geflossen, und der Sieg ist auf unserer Seite geblieben. Es handelt sich darum, diesen Sieg an unsre Fahne zu ketten. Und dazu bedürfen wir der richtigen Männer, die sich jeden Augenblick bewußt sind, daß das deutsche Gemüt einer Niedrigkeit nicht fähig ist. Und Verrat an unsren heiligsten Gütern ist Niedrigkeit. Unter uns, das weiß ich, ist niemand. Aber nicht alle denken und fühlen so, da sind ihrer noch viele, die der Freiheit nach dem Leben trachten. Mit Geierschnäbeln hacken sie danach. Ich bin deshalb für Anschluß an Frankreich und sehe Gefahr für Preußen in jenem Mann, der Polen eingesargt hat und unsre junge Freiheit nicht will. Also, meine Herren, Männer von verbürgter Königs-, aber zugleich auch von verbürgter Volkstreue: Jahn, Arndt, Boyen, Grolmann, vielleicht auch Pfuel. Die werden unsre Fahne hochhalten. Ich wähle Humboldt.«

Die Rede wurde mit Beifallsgemurmel aufgenommen, und nur der Vorsitzende lächelte. Zu Widerlegungen sah er sich aber nicht gemüßigt, und so fiel mir Ärmsten denn die Aufgabe zu, dem einem allerhöchsten Ziele wild nachjagenden Schulvorsteher in die Zügel zu fallen. Sehr gegen meine Neigung. Ich war über dies öde, wichtigtuerische Papelwerk aufrichtig indigniert und bemerkte dementsprechend mit einer gewissen übermütigen Emphase, daß uns hier nicht zubestimmt sei, für die Hohenzollern oder für die Freiheit direkte Sorge zu tragen, sondern daß wir hier in der Gotteswelt weiter nichts zu tun hätten, als in unsrer Eigenschaft als bescheidene Urwähler einen bescheidenen Wahlmann zu wählen. All das andre käme nachher erst; da sei dann der Augenblick da, Preußen nach rechts oder nach links zu leiten. Hoffentlich nach links. Ich müßte deshalb auch darauf verzichten, Alexander von Humboldt an dieser Stelle meine

Stimme zu geben, und wäre vielmehr für meinen Nachbar Bäcker Roesike, von dem ich wüßte, daß er ein allgemein geachteter Mann sei und in der ganzen Gegend die besten Semmeln hätte.

Da zufällig kein andrer Bäcker zugegen war, so war man mit meinem Vorschlag allgemein einverstanden; aber Roesike selbst, allem Ehrgeiz fremd, wollte von seiner Wahl nichts wissen, schlug vielmehr in verbindlicher Revanche *mich* vor, und als wir zehn Minuten später das Wahllokal verließen, war ich in der Tat *Wahlmann*.

Dies war mein Debüt auf dem Wollboden, zugleich erstes und letztes Auftreten als Politiker.

Am Abend ebendieses Tages ging ich nach Bethanien hinaus, um dort dem Pastor Schultz, mit dem ich, trotz weitestgehender politischer und kirchlicher Gegensätze, befreundet war, einen Besuch zu machen. Als ich draußen ankam, sah ich an den im Vorflur an verschiedenen Riegeln und Haken hängenden Hüten und Sommerüberziehern, daß drinnen im Schultzschen Wohnzimmer Besuch sein müsse. Das war mir nicht angenehm. Aber was half es, und so trat ich denn ein. Um einen großen, runden Tisch herum saßen sechs oder sieben Herren, lauter Pommersche von Adel, unter ihnen ein Senfft-Pilsach, ein Kleist, ein Dewitz. Aus ein paar Worten, die gerade fielen, als ich eintrat, konnte ich unschwer heraushören, daß man über die Wahlen sprach und sich darüber mokierte. Schultz, sonst ein sehr ernster Mann – *zu* ernst –, war der ausgelassenste von allen, und als er mich von der Tür her meine Verbeugung gegen die Herren machen sah, rief er mir übermütig zu: »Was führt dich her! Du bist am Ende Wahlmann geworden.«

Ich nickte.

»Natürlich. So siehst du auch gerade aus.«

Alles lachte, und ich hielt es für das klügste, mit einzustimmen, trotzdem ich, ein bißchen ingrimmig in meiner Seele, das eitle Gefühl hatte: »Lieber Schultz, mit *dir* nehm ich es auch noch auf.«

x ist in Beziehung auf die Coefficienten von $f(\alpha)^\lambda$ vom zweiten Grade. Auch läßt sich x durch die Coefficienten von $\psi_1(\alpha)$ $\psi_2(\alpha)$ etc. wo $\psi_r(\alpha) = \frac{(\alpha, x)(\alpha', x)}{(\alpha^{r+1}, x)}$ ausdrücken und zwar als lineäre Function derselben. Ich ziehe aber den Ausdruck durch die Coefficienten von $f(\alpha)^\lambda$ vor.

Da ich nun diesen nicht unwichtigen Punkt erobert und der Herrschaft der Wissenschaft unterthänig gemacht habe, so können Sie sich denken, daß ich jetzt versuche von hier aus weiter gegen meinen Hauptfeind, das simple Reciprocitätsgesetz, zu operiren. Es fehlt mir auch nicht an Muth dazu, da ich durch die bisherigen Erfolge kühner gemacht worden bin, und da ich mir bewußt bin bis jetzt noch täglich an der gründlicheren Kenntnis meines Gegenstandes zu gewinnen.

... Leben Sie wohl, empfehlen Sie mich Ihrer Fräulein Braut und den Ihrigen allen und kommen Sie ja recht bald zu Ihrem Freunde

E. KUMMER.

Breslau d. 5. Maj 1848.

... Können Sie sich wohl vorstellen, daß ich seit acht Tagen mich zweimal als Volksredner versucht habe? Bei einer Versammlung unseres Wahlbezirks trat ich zuerst auf, und sprach über die Eigenschaften eines guten Wahlmannes, welches sehr großen Anklang fand. Ich wurde darauf einstimmig zum Vorsitzenden für die nächste Versammlung gewählt. Auch hatte ich bei dieser ersten Versammlung mein Terrain recognoscirt und gefunden, daß der demokratische Klubb ganz dominierte und zwar nur durch unbedeutende Personen, welche sich zu Wahlmännern aufwerfen wollten. Diese schmeichelten den Arbeitern um zu reüssiren, verdächtigten die Beamten und gebrauchten alle die gewöhnlichen Kunstgriffe. Ich faßte darum den Entschluß wenigstens einen dieser Leute durch meine Person zu verdrängen und hielt in der zweiten Versammlung eine zweite Rede vorzüglich an die Arbeiter gerichtet. Obgleich ich nun gerade die entgegengesetzten Mittel anwendete, als jene Demokraten, nämlich den Arbeitern zu zeigen, was sie seit dem 18. März wirklich erreicht hätten, und ihnen Vertrauen zu der gegenwärtigen Regierung einzuflößen, so reüssirte ich doch vollständig. Die Demokraten hielten zwar noch eine Versammlung am Sonntage, wo sie mich zu verdrängen suchten, es gelang ihnen aber nicht, wie Sie aus der Liste der Wahlmänner ersehen haben. Neben mir sind außer zwei hiesigen Bürgern allerdings nur Mitglieder

des demokratischen Klubbs für Berlin und Frankfurt gewählt worden; überhaupt haben die Demokraten hier durchgängig gesiegt. Ich selbst bin auch gar nicht gegen die Demokraten überhaupt eingenommen, wenn sie es nur gegenwärtig mit der Befestigung einer durchaus freisinnigen constitutionellen Monarchie redlich meinen, und nicht gegen das Königthum zu Felde ziehen, auch nicht streben es heimlich zu untergraben, so sind mir die Demokraten im Grunde lieber als die philisterhaften Bürger, welche an den Wahlen für Frankfurt fast gar nicht mehr Theil nahmen, weil sie für diese wenig oder gar kein Interesse hatten. Die Anforderungen, die ich an einen Deputirten nach Berlin stelle sind 1. wahre Vaterlandsliebe, 2. Einsicht und Verstand, 3. Charakterfestigkeit. Speciellere Anforderungen stelle ich nicht, weil wir die Candidaten nehmen müssen wie sie eben zuletzt bei den engeren und engsten Wahlen übrig bleiben. Wohl uns, wenn wir zuletzt aus zwei guten den besten wählen können, es kann aber auch kommen, daß wir zuletzt aus zwei Uebeln noch das geringere zu wählen haben. Für einen Deputirten nach Frankfurt würden die Anforderungen dieselben sein, nur daß seine Vaterlandsliebe mehr in dem einigen Deutschland als in Preußen ihre Hauptwurzel haben müsse, und daß auch seine Einsicht sich mehr auf das allgemeinere erstrecken möchte. — Ich bin auf meine Würde als Wahlmann sehr stolz wie Sie daraus ersehen können, daß ich mich in Fürstenstein, wo wir am Mittwoch waren, als E. KUMMER, Wahlmann eingeschrieben habe, meine Frau als Wahlweib, den Vetter als Urwähler und LOUISE CAUER als Wahlverwandtschaft. Ich freue mich aber wirklich, daß es mir gelungen ist, besonders darum weil mich nur wahrer Patriotismus dazu vermocht hat meine Schüchternheit zu überwinden, und als Redner vor einer solchen gemischten Versammlung aufzutreten. Sobald ich meinen Pflichten als Bürger werde genügt haben, nämlich unmittelbar nach den Wahlen für die Frankfurter Versammlung, werde ich sogleich wieder meine mathematischen Arbeiten mit voller Kraft vornehmen, denn dann habe ich für Politik für den Augenblick nichts weiter zu thun. Wenn Sie mich in nächster Woche besuchen, worauf ich mich sehr freue so erzähle ich Ihnen das nähere über die hiesigen Wahlen und will Ihnen auch das Concept meiner ersten Rede mittheilen, die zweite war fast ganz frei gesprochen, und nur im allgemeinen prämeditirt. Leben Sie wohl, . . . und empfangen Sie . . . die herzlichsten Grüße der meinigen

Ihr Sie herzlich liebender Freund

E. KUMMER.

6*

DER ACHTZEHNTE MÄRZ

FÜNFTES KAPITEL

Nachspiel — Berlin im Mai und Juni 48

Ich habe, voraufgehend, von meiner Wahlmannschaft und einer gleichzeitigen oratorischen Leistung auf dem in der Neuen Königstraße gelegenen Wollboden als von meinem »ersten und letzten Auftreten als Politiker« gesprochen. Es war das auch im wesentlichen richtig. Ich habe jedoch hinzuzufügen, daß diesem »ersten und letzten Auftreten« noch ein mit zur Sache gehöriges *Nachspiel* folgte. Dies Nachspiel waren die Wahlmännerversammlungen behufs Wahl eines Abgeordneten. Auf dem Wollboden in der Neuen Königstraße war ich gewählt *worden,* im Konzertsaale des Königlichen Schauspielhauses, wo die Wahlmännerversammlungen stattfanden, *hatte* ich zu wählen oder mich wenigstens an den Beratungen zu beteiligen. Das tat ich denn auch, und ich zähle die Stunden, in denen die Beratungen stattfanden, zu meinen allerglücklichsten. Es war alles voll Leben und Interesse, wenn auch, aufs eigentlich Politische hin angesehen, jeder moderne Parlamentarier sich schaudernd davon abwenden würde. Gerade von den besten Männern wurden Dinge gesprochen, die kaum in irgendwelcher Beziehung zu dem dort zu Verhandelnden standen; aber so sonderbar und oft das Komische streifend diese spontan abgegebenen und sehr »in die Fichten« gehenden Schüsse wirkten, so war doch in diesen dilettantischen Expektorationen immer »was drin«. So sprach einmal der alte General *Reyher* – Chef des Großen Generalstabes und Vorgänger Moltkes, welcher letztere sich später oft dankbar zu diesem seinem Lehrer bekannt hat – und legte ganz kurz ein politisches, mit Rücksicht auf die Dinge, zu deren Erledigung wir versammelt waren, völlig zweckloses Glaubensbekenntnis ab. Es machte aber doch einen großen Eindruck auf mich, einen alten, würdigen General sich freimütig zu seinem König und zur Armee bekennen zu hören. Denn von derlei Dingen hörte man damals wenig. Und dann, ich glaube, es war an demselben Tage, schritt der alte *Jakob Grimm* auf das Podium zu, der wundervolle Charakterkopf – ähnlich wie der Kopf

DER ACHTZEHNTE MÄRZ

Mommsens sich dem Gedächtnis einprägend –, von langem, schneeweißem Haar umleuchtet, und sprach irgend etwas von Deutschland, etwas ganz Allgemeines, das ihm in jeder richtigen politischen Versammlung den Ruf: »Zur Sache« eingetragen haben würde. Dieser Ruf unterblieb aber, denn jeder war betroffen und gerührt von dem Anblick und fühlte, wie weitab das alles auch liegen mochte, daß man ihm folgen müsse, wollend oder nicht.

Das waren so zwei glänzende, mir durch alle Zeit hin in Erinnerung gebliebene Gestalten, während die meisten freilich nur Schwätzer und Nullen waren, ein paar auch sogar Hochstapler. Ich kenne noch ganz gut ihre Namen, aber ich werde mich hüten, sie hier zu nennen.

Wie lange diese Sitzungen dauerten, weiß ich nicht mehr; ich weiß nur, daß alles, was ich erlebte, mich tagtäglich beglückte: der schöne Saal, das herrliche Wetter – wie's ein Hohenzollernwetter gibt, so gibt es auch ein Revolutionswetter –, der Verkehr, das Geplauder. Eine Befangenheit, zu der ich sonst wohl neige, kam nicht auf, weil niemand da war – selbst die besten mit eingerechnet, denen dann eben wieder das Politische fehlte –, der mir hätte imponieren können. Von meiner Unausreichendheit, meinem Nichtwissen tief durchdrungen, sah ich doch deutlich, daß, kaum zu glauben, das Nichtwissen der andern womöglich noch größer war als das meinige. So war ich bescheiden und unbescheiden zugleich.

Eines Tages, als ich aus einer dieser immer den halben Tag wegnehmenden Sitzungen nach meiner Neuen Königstraße zurückkehrte, fand ich daselbst ein Billett vor, dessen Aufschrift ich rasch entnahm, daß es von meinem Freunde, dem schon im vorigen Kapitel genannten Pastor Schultz in Bethanien, herrühren müsse. So war es denn auch. Er fragte ganz kurz bei mir an, ob ich vielleicht bereit sei, die pharmazeutisch-wissenschaftliche Ausbildung zweier bethanischer Schwestern zu übernehmen, da man gewillt sei, den bethanischen Apothekendienst in die Hände von Diakonissinnen zu legen. Im Falle dieser sein Antrag mir passe, wäre es erwünscht, wenn ich baldmöglichst in die betreffende Stellung einträte. Das war eine ungeheure Freude. Auskömm-

Lecture 8 [Lecture 16]

Kummer on Fermat's theorem

We return to $\mathbf{Z}(\alpha)$, at first for α a cube-root of 1, thus the solution

$$\alpha = \cos(2\pi/3) + i\sin(2\pi/3)$$

of

$$z^2 + z + 1 = 0.$$

We saw that if p is a prime number that leaves the remainder 3 on division by 3, then there is an integer a such that $a^2 + a + 1$ is divisible by p. We considered the greatest common divisor of $a - \alpha$ and p and discovered that it had to be a number π such that $p = \pi\overline{\pi}$, thus it is one of the two factors of p.

Suppose now that n is any odd prime and that we take α to be

$$\alpha = \cos(2\pi/n) + i\sin(2\pi/n),$$

thus a root of

$$Z^{n-1} + Z^{n-2} + \cdots + Z + 1 = 0.$$

The domain $\mathbf{Z}(\alpha)$ now consists of all numbers

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-2}\alpha^{n-2},$$

where the coefficients $a_0, a_1, \ldots, a_{n-2}$ are integers, thus ordinary whole numbers.

Now just as we showed that for $n = 3$ and $p \equiv 1 \pmod 3$, there is always an integer a such that $a^2 + a + 1$ is divisible by p, we can show that if p leaves the remainder 1 upon division by n, then there is an integer a such that

$$a^{n-2} + a^{n-3} + \cdots + a^2 + a + 1$$

is divisible by p. If the domain $\mathbf{Z}(\alpha)$ possessed unique factorization, we could expect that the greatest common divisor of $a - \alpha$ and p was again a prime divisor π of p.

More precisely, there are $n - 1$ symmetries of the domain $\mathbf{Z}(\alpha)$, determined by

$$\begin{aligned}
\sigma_1 &: \alpha \to \alpha, \\
\sigma_2 &: \alpha \to \alpha^2, \\
\sigma_3 &: \alpha \to \alpha^3, \\
&\vdots \\
\sigma_{n-1} &: \alpha \to \alpha^{n-1},
\end{aligned}$$

The norm of a number ξ is defined to be

$$\xi \cdot \sigma_2(\xi)\sigma_3(\xi)\cdots\sigma_{n-1}(\xi).$$

Date of lecture: Spring term, March 21, 2000.

We can even expect that

$$\mathrm{N}\,\pi = \pm p.$$

Kummer's first papers were on differential equations and infinite series, but in one of his earliest papers on cyclotomy, he, on the assumption that unique factorization exists in each domain $\mathbf{Z}(\alpha)$, set about finding π for each p. In a paper, written for a formal occasion and thus in Latin, on the complex numbers formed from roots of unity and whole numbers, thus on the domain $\mathbf{Z}(\alpha)$, he sets about calculating π for p up to 1,000 that leave the remainder 1 upon division by n. The first values of n are 3, 5, 7, 11, 13, 17, 19 and 23. Of course, if the domain does not possess unique factorization, then his calculation will not lead to a well-defined result. He will not always arrive at a well-defined greatest common divisor; he will not always arrive at a number whose norm is p; and he will not always find a factorization of p into primes of the domain $\mathbf{Z}(\alpha)$. He tabulates his results, from which we see in particular that for $n = 23$, there are five primes less than 1,000 that cannot be factored.

The numbers in $\mathbf{Z}(\alpha)$ beside the five last primes in Kummer's tables have the following norms.

47	47^2
139	139^2
277	$277 \cdot 17159$
461	$47 \cdot 967$
967	967^2

It appears that Kummer put the wrong element of $\mathbf{Z}(\alpha)$ on the fourth line. Perhaps someone would like to find the right one. The necessary calculations are far easier now than in his day. Curiously, some reader, of the original journal article not of the collected works, appears to have corrected the preceding line. The point is that these last five numbers are exceptions. He is unable to find numbers in $\mathbf{Z}(\alpha)$ of which any of these five numbers are norms. Their squares or sometimes the products of two of them are, however, sometimes norms.

(1) Si $\lambda = 5$, et α radix æquationis $\alpha^5 = 1$.

$11 = N(2+\alpha)$
$31 = N(2-\alpha)$
$41 = N(3+2\alpha+\alpha^2)$
$61 = N(3+\alpha)$
$71 = N(3-\alpha+\alpha^2)$
$101 = N(3+\alpha-\alpha^2)$
$131 = N(3+\alpha-\alpha^4)$
$151 = N(3+2\alpha-\alpha^4)$
$181 = N(4+3\alpha)$
$191 = N(4+\alpha+2\alpha^2)$
$211 = N(3-2\alpha)$
$241 = N(4-\alpha+\alpha^2)$
$251 = N(5+2\alpha+\alpha^4)$
$271 = N(3-3\alpha+\alpha^2)$
$281 = N(4-\alpha-\alpha^2)$
$311 = N(3+2\alpha+2\alpha^2+\alpha^3)$
$331 = N(4-2\alpha+\alpha^2)$
$401 = N(4+3\alpha-\alpha^4)$
$421 = N(5+2\alpha+2\alpha^2)$
$431 = N(4-2\alpha-\alpha^4)$
$461 = N(4-\alpha-\alpha^3)$
$491 = N(5+3\alpha+\alpha^3)$
$521 = N(5+\alpha^3)$
$541 = N(3-3\alpha-\alpha^3)$
$571 = N(6+5\alpha+3\alpha^2)$
$601 = N(5+2\alpha-\alpha^2)$
$631 = N(4-2\alpha-\alpha^3)$
$641 = N(5+3\alpha+4\alpha^2)$
$661 = N(5+\alpha-\alpha^2+3\alpha^3)$
$691 = N(3-3\alpha-2\alpha^2)$
$701 = N(4-\alpha-2\alpha^2+\alpha^3)$
$751 = N(6+4\alpha+3\alpha^2)$
$761 = N(5-2\alpha+\alpha^2)$
$811 = N(3-3\alpha-2\alpha^2+\alpha^3)$
$821 = N(4-\alpha-2\alpha^2+2\alpha^3)$
$881 = N(6+2\alpha+\alpha^2)$
$911 = N(5+\alpha^2-2\alpha^4)$
$941 = N(4+3\alpha-3\alpha^2-\alpha^3)$
$971 = N(5-2\alpha-\alpha^4)$
$991 = N(6+\alpha+\alpha^3)$

(2) Si $\lambda = 7$, et α est radix æquationis $\alpha^7 = 1$.

$29 = N(1+\alpha-\alpha^3)$
$43 = N(2+\alpha)$
$71 = N(2+\alpha+\alpha^3)$
$113 = N(2-\alpha+\alpha^3)$
$127 = N(2-\alpha)$
$197 = N(3+\alpha+\alpha^3+\alpha^6)$
$211 = N(3+\alpha+2\alpha^2)$
$239 = N(3+2\alpha+2\alpha^2+\alpha^3)$
$281 = N(2-\alpha-2\alpha^3)$
$337 = N(2+\alpha-\alpha^2-\alpha^4)$
$379 = N(3+2\alpha+\alpha^2)$
$421 = N(3+\alpha+\alpha^2)$
$449 = N(2+\alpha-\alpha^3-\alpha^6)$
$463 = N(3+2\alpha)$
$491 = N(3+\alpha+\alpha^2-\alpha^3)$
$547 = N(3+\alpha)$
$617 = N(2+\alpha+\alpha^2-\alpha^5)$
$631 = N(2+2\alpha-\alpha^2+\alpha^3+\alpha^6)$

$659 = N(2 + 2\alpha - \alpha^2 + \alpha^3)$
$673 = N(4 + 3\alpha + 2\alpha^2 + \alpha^4 + 2\alpha^6)$
$701 = N(3 + \alpha + \alpha^4 - \alpha^5 + \alpha^6)$
$743 = N(3 + 2\alpha - \alpha^3 - \alpha^4)$
$757 = N(3 + 2\alpha + \alpha^3)$
$827 = N(2 + 2\alpha - \alpha^4 - \alpha^5)$
$883 = N(2 - \alpha^2 - 2\alpha^3 - \alpha^5)$
$911 = N(3 + 2\alpha - \alpha^3 + \alpha^4)$
$953 = N(3 + \alpha - \alpha^2 - \alpha^3)$
$967 = N(2 + 2\alpha - \alpha^3 + 2\alpha^5)$

(3) Si $\lambda = 11$, et α est radix æquationis $\alpha^{11} = 1$.

$23 = N(1 + \alpha + \alpha^2)$
$67 = N(1 + \alpha + \alpha^2 + \alpha^4 + \alpha^5)$
$89 = N(1 + \alpha + \alpha^4 + \alpha^6)$
$199 = N(1 + \alpha - \alpha^2)$
$331 = N(1 - \alpha + \alpha^3 + \alpha^5)$
$353 = N(1 + \alpha + \alpha^3 + \alpha^4 - \alpha^7)$
$397 = N(1 + \alpha + \alpha^6 - \alpha^7)$
$419 = N(1 + \alpha - \alpha^2 + \alpha^3)$
$463 = N(1 - \alpha - \alpha^2 + \alpha^3 + \alpha^5)$
$617 = N(2 + \alpha + \alpha^7 + \alpha^{10})$
$661 = N(1 + \alpha - \alpha^2 + \alpha^4 - \alpha^5)$
$683 = N(2 + \alpha)$
$727 = N(1 + \alpha + \alpha^2 - \alpha^3 - \alpha^4)$
$859 = N(1 + \alpha + \alpha^2 + \alpha^3 + \alpha^7 - \alpha^8)$
$881 = N(1 + \alpha + \alpha^2 + \alpha^3 - \alpha^4 - \alpha^7 - \alpha^8)$
$947 = N(2 + \alpha^3 - \alpha^4 - \alpha^6)$
$991 = N(2 + \alpha + \alpha^3)$

(4) Si $\lambda = 13$, et α est radix æquationis $\alpha^{13} = 1$.

$53 = N(1 + \alpha + \alpha^3)$
$79 = N(1 - \alpha + \alpha^{10})$
$131 = N(1 - \alpha + \alpha^{11})$
$157 = N(1 + \alpha + \alpha^2 + \alpha^3)$
$313 = N(1 - \alpha + \alpha^3 + \alpha^6)$
$443 = N(1 + \alpha - \alpha^3 + \alpha^8)$
$521 = N(1 + \alpha - \alpha^{12})$
$547 = N(1 - \alpha - \alpha^2 + \alpha^3 + \alpha^6)$
$599 = N(1 + \alpha - \alpha^7 + \alpha^8 + \alpha^{11})$
$677 = N(1 - \alpha - \alpha^4 + \alpha^6 + \alpha^7)$
$959 = N(1 + \alpha - \alpha^2 - \alpha^3 + \alpha^7)$
$911 = N(1 + \alpha^3 + \alpha^5 - \alpha^7 - \alpha^{11})$
$937 = N(1 + \alpha^3 - \alpha^7 + \alpha^8 - \alpha^{10})$

(5) Si $\lambda = 17$, et α est radix æquationis $\alpha^{17} = 1$.

$103 = N(1 + \alpha^2 + \alpha^3)$
$137 = N(1 + \alpha - \alpha^3)$
$239 = N(1 + \alpha + \alpha^3)$
$307 = N(1 - \alpha + \alpha^2)$
$409 = N(1 - \alpha^2 + \alpha^3)$
$443 = N(1 + \alpha + \alpha^2 + \alpha^3 - \alpha^{15})$
$613 = N(1 + \alpha^2 - \alpha^3)$
$647 = N(1 + \alpha + \alpha^{13} + \alpha^{15})$
$919 = N(1 + \alpha + \alpha^3 - \alpha^5 + \alpha^7)$
$953 = N(1 + \alpha + \alpha^3 - \alpha^{13})$

(6) Si $\lambda = 19$, et α est radix æquationis $\alpha^{19} = 1$.

$191 = N(1 + \alpha + \alpha^{16})$ $\qquad$ $457 = N(1 + \alpha + \alpha^3)$

$229 = N(1 - \alpha - \alpha^5)$ $\qquad$ $571 = N(1 + \alpha + \alpha^2 + \alpha^3 - \alpha^5)$

$419 = N(1 + \alpha - \alpha^2)$ $\qquad$ $647 = N(1 - \alpha^2 + \alpha^9)$

$761 = N(1 - \alpha^2 + \alpha^{12})$

(7) Si $\lambda = 23$, et α est radix æquationis $\alpha^{23} = 1$.

$599 = N(1 + \alpha^5 - \alpha^6)$ $\qquad$ $691 = N(1 + \alpha + \alpha^5)$

$829 = N(1 + \alpha^{11} + \alpha^{20})$

Reliqui numeri primi formæ $23m + 1$ infra mille undecim factoribus primis constant, habet

47 factorem $\alpha^{10} + \alpha^{13} + \alpha^5 + \alpha^{15} + \alpha^7 + \alpha^{16}$

139 » $\alpha^{10} + \alpha^{12} + \alpha^3 + \alpha^{13} + \alpha^4 + \alpha^{17}$

277 » $2 + \alpha + \alpha^{21} + \alpha^7 + \alpha^{16}$

461 » $\alpha + \alpha^{22} + \alpha^{16} + \alpha^{12} + \alpha^8 + \alpha^{15} + \alpha^9 + \alpha^{14}$

967 » $2 + \alpha^{11} + \alpha^{17} + \alpha^4 + \alpha^{19}$.

§ XI.

Quæ de numeris complexis et de eorum factoribus primis commentati sumus ad doctrinam de sectione circuli felicissimo successu applicari possunt. In hac enim doctrina tales numeri complexi eorumque producta maximi momenti sunt, quorum vera indoles in luce clarissima ponitur si in factores primos diffinduntur.

Sit p numerus primus realis formæ $m\lambda + 1$, α radix imaginaria æquationis $\alpha^{\lambda} = 1$, g radix primitiva numeri primi p, et

$$(\alpha, x) = x + \alpha x^g + \alpha^2 x^{g^2} + \ldots + \alpha^{p-2} x^{g^{p-2}}$$

Totius fere doctrinæ de circuli sectione caput est formæ hujus (α, x) potestas exponentis λ, quæ a radice x non pendet, sed radicis α functio rationalis integra est, ideoque numerus complexus ejus generis quod supra tractavimus. Ipsa hæc formula (α, x), quam Cl. Lagrange primus adhibuit, proprietatibus insignibus gaudet, quarum maximas Cl. Jacobi primus invenit

$$(\alpha, x)(\alpha^{-1}, x) = p,$$

$$\frac{(\alpha^m, x)(\alpha^n, x)}{(\alpha^{m+n}, x)} = \psi(\alpha) = A + A_1\alpha + A_2\alpha^2 + \ldots + A_{\lambda-1}\alpha^{\lambda-1},$$

Maxime dolendum videtur, quod hæc numerorum realium virtus, ut in tactores primos dissolvi possint, qui pro eodem numero semper iidem sint, non eadem est numerorum complexorum, quæ si esset, tota hæc doctrina, quæ magnis adhuc difficultatibus laborat, facile absolvi et ad finem perduci posset. Eam ipsam ob causam numeri complexi, quos hic tractamus, imperfecti esse videntur, et dubium inde oriri posset, utrum hi numeri complexis ceteris qui fingi possint præferendi, an alii quærendi essent, qui in hac re fundamentali analogiam cum numeris integris realibus servarent. Attamen hi numeri complexi, qui unitatis radicibus et numeris integris realibus componuntur, non ex arbitrio facti sunt, sed ex ipsa doctrina numerorum procreati, atque ipsorum ea ratio est, ut in doctrina sectionis circuli et residuorum potestatum altiorum ulterius promovenda iis carere nullo modo possimus.

De numeris complexis, qui radicibus unitatis et numeris integris realibus constant

Citation.

> We see with great sorrow that that virtue of ordinary numbers, that they can be resolved into prime factors that for the same number are always the same, is not possessed by complex numbers. If it were, all the theory, that is so far beset with great difficulties, would be easy to develop and to bring to completion. For this reason the complex numbers that we treat here are seen to be imperfect, so that a doubt could arise, whether other complex numbers that might be constructed are preferable, whether there are others to be investigated that in this fundamental respect would preserve the analogy with ordinary integers. Nevertheless those complex numbers that are composed from roots of unity and ordinary integers are not constructed arbitrarily, but are generated by the theory of numbers itself, which is indeed their very source, so that in developing the theory of cyclotomy and of the residues of higher powers we can in no manner neglect them.

Kummer saves the day with the introduction of *ideal* factors. I shall not give his definition, but a more modern one, which is simpler, but the wonder and brilliance is gone. The proofs are also then farther to seek. I introduce the modern definition out of expediency. We have little time left. If ξ is any number in $\mathbf{Z}(\alpha)$, then the collection of numbers $\mu\xi$, μ being any other number in $\mathbf{Z}(\alpha)$ is such that if η and ζ are in this collection, then so are $\eta + \zeta$ and $\nu\eta$, ν being an arbitrary number in $\mathbf{Z}(\alpha)$. Thus

$$\mu_1\xi + \mu_2\xi = (\mu_1 + \mu_2)\xi, \tag{A}$$

and

$$\nu(\mu\xi) = (\mu\nu)\xi. \tag{B}$$

Our experience with the Euclidean algorithm, suggests that if, on the other hand, we have any collection of numbers with the properties (A) and (B), then it is in fact just the collection of multiples of some ξ by the numbers of $\mathbf{Z}(\alpha)$. Our experience is of course limited and leads to the wrong conclusion, but what we can do is introduce for any collection satisfying (A) and (B) an ideal number, of whose multiples the collection is imagined to exist. The value of these ideal numbers is determined by the useful properties they possess. Notice that every number in $\mathbf{Z}(\alpha)$ determines an ideal number: the collection of all its multiples. Moreover two numbers in $\mathbf{Z}(\alpha)$ determine the same ideal number if and only if they differ by a unit. Moreover $\mathbf{Z}(\alpha)$ itself is an ideal number, the collection of multiples of 1.

They can be multiplied. If $\mathfrak{a} = \{\mu\}$ and $\mathfrak{b} = \{\nu\}$ are two ideal numbers, then $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ consists of all numbers

$$\mu_1\nu_1 + \mu_2\nu_2 + \cdots,$$

the number of terms being arbitrary, but of course finite, and μ_i lying in $\mathfrak{a}$ and ν_i lying in $\mathfrak{b}$. If $\mathfrak{a}$ were just the multiples of ξ and $\mathfrak{b}$ just the multiples of η, then $\mathfrak{c}$ would just be the multiples of $\xi\eta$. If we multiply an ideal number by 1, thus by $\mathbf{Z}(\alpha)$, we just obtain the ideal number itself back. This said, the notion of a prime

ideal number is clear. An ideal number is prime if when it is the product of two other ideal numbers, one of these numbers is 1 and the other necessarily then the ideal itself.

Kummer proves, first of all, that every number has a unique factorization into ideal numbers, and expresses this theorem with a chemical analogy. We might suggest nowadays that ideal numbers are like the physicists quarks, however Kummer's analogy is more explicit and reflects better his actual construction:

> I have discussed the ideal factors at length with Dirichlet and more briefly with Jacobi. I used a symbolic expression taken from chemistry: the prime factors are the elements, the ideal prime factors are those elements that do not appear alone, but only in combination with other elements, equivalent complex ideal numbers are as such the same as equivalent combining proportions of the chemical ingredients.[2] The search for the ideal prime factors is the chemical analysis, the complex numbers labelled ψ or Ψ in my essay are the reagents and the whole number q, which appears as a real factor, is the sediment that manifests itself upon application of the right reagent. In brief, the whole collection of notions of chemistry agrees in a striking fashion with those in which the theory of complex numbers is formulated.

Two ideal numbers $\mathfrak{a}$ and $\mathfrak{b}$ are called equivalent if there are ordinary numbers a and b in $\mathbf{Z}(\alpha)$ such that $a\mathfrak{a} = b\mathfrak{b}$. If $\mathfrak{a}$ is equivalent to $\mathfrak{b}$ and $\mathfrak{b}$ to $\mathfrak{c}$, then, as is to be expected, $\mathfrak{a}$ is equivalent to $\mathfrak{c}$. Thus the collection of all ideal numbers is decomposed into classes, one class being formed of all ideal numbers equivalent to any given one. One very important fact (or theorem) established by Kummer right at the beginning of his investigations is that the number of different classes is finite.

He also investigates, and this is easier, the units. I observe that there are very many units in $\mathbf{Z}(\alpha)$ if n is larger than 3. Some can be formed in the following way. If $1 < r < \ell$, then

$$\frac{1-\alpha^r}{1-\alpha} = 1 + \alpha + \alpha^2 + \cdots + \alpha^{r-2} + \alpha^{r-1}$$

is in $\mathbf{Z}(\alpha)$. If we choose s such that $rs \equiv 1 \pmod{\ell}$ and apply the symmetry $\alpha \to \alpha^s$, then this relation becomes

$$\frac{1-\alpha}{1-\alpha^s} = 1 + \alpha^s + \alpha^{2s} + \cdots + \alpha^{(r-2)s} + \alpha^{(r-1)s},$$

[2]My limited knowledge of chemistry and of chemical terms in any language forces me to guess here. I suppose that two different molecules can be combined of the same elements in the same proportions, and that the reference is to this, but I do not know and would be happy for a correction or a confirmation.

Uebermorgen, als den Mondtag gehen meine Vorlesungen an und zwar gleich drei auf einmal zu denen ich mich noch präpariren soll, was bei dem Anfange allemal Schwierigkeiten hat, wenn man sich nicht gleich in medias res hineinstürzen will oder kann.

Leben Sie recht wohl

Ihr

E. KUMMER.

Breslau d. 14. Juni 1846.

Herzlich geliebter Freund!

. . . Ueber die idealen Factoren habe ich mehreres mit DIRICHLET und einiges mit JACOBI verhandelt. Ich gebrauchte dabei immer die bildliche Ausdrucksweise, aus der Chemie entnommen: Die Primfactoren sind die Elemente, die idealen Primfactoren sind diejenigen Elemente welche nicht für sich darstellbar nur in Verbindung mit anderen vorkommen, äquivalente complexe ideale Zahlen sind an sich dasselbe als äquivalente Gewichtsmengen der chemischen Stoffe. Die Aufsuchung der idealen Primfactoren ist die chemische Analyse, die in meinem Aufsatze mit ψ oder Ψ bezeichneten complexen Zahlen sind die Reagentien und die ganze Zahl q, welche als realer Factor heraustritt, ist der Niederschlag welcher nach Anwendung des richtigen Reagens sich zeigt. Kurz die ganze Begriffssphäre der Chemie stimmt auf eine eclatante Weise mit derjenigen zusammen in welcher sich die Lehre von den complexen Zahlen bewegt. DIRICHLET hat mich sehr ermahnt die Theorie bald fertig auszuarbeiten und CRELLE zum Drucke zu übergeben. Auch hat er mir erzählt und gezeigt, nämlich aus mündlichen und schriftlichen Aeußerungen von GAUSS, daß GAUSS schon bei Anfertigung des Abschnittes de compositione formarum aus den Disqu. arith. etwas ähnliches wie ideale Factoren zu seinem Privatgebrauche gehabt hat, daß er dieselben aber nicht auf sicheren Grund zurückgeführt hat, er sagt nämlich in einer Note seiner Abhandlung über die Zerfällung der ganzen rat. Functionen in lineäre Factoren ohngefähr so: „Wenn ich hätte auf dieselbe Weise verfahren wollen wie die früheren Mathematiker mit dem imaginären, so würde eine andere meiner Untersuchungen die sehr schwierig ist sich auf sehr leichte Weise haben machen lassen.“ Daß hier die compositio formarum gemeint ist, hat DIRICHLET später mündlich von GAUSS erfahren. Ich habe ferner DIRICHLET meine Vermuthung mitgetheilt daß zwischen

hat. Der chemischen Verbindung entspricht für die complexen Zahlen die Multiplication; den Elementen, oder eigentlich den Atomgewichten derselben, entsprechen die Primfactoren; und die chemischen Formeln für die Zerlegung der Körper sind genau dieselben, wie die Formeln für die Zerlegung der Zahlen. Auch selbst die idealen Zahlen unserer Theorie finden sich in der Chemie, vielleicht nur allzuoft, als hypothetische Radicale, welche bisher noch nicht dargestellt worden sind, die aber, so wie die idealen Zahlen, in den Zusammensetzungen ihre Wirklichkeit haben. Das Fluor, für sich bisher nicht darstellbar und noch den Elementen zugezählt, kann als Analogon eines idealen Primfactors gelten. Die Idealität in der Chemie verhält sich aber darin wesentlich anders, als die der complexen Zahlen, dafs chemische ideale Stoffe, mit wirklichen verbunden, auch wirkliche Stoffe produciren; was bei den idealen Zahlen nicht der Fall ist. In der Chemie hat man ferner zur Prüfung der in einem unbekannten aufgelöseten Körper enthaltenen Stoffe die Reagentien, welche Niederschläge geben, aus denen die Anwesenheit der verschiedenen Stoffe sich erkennen läfst. Ganz Dasselbe findet für die complexen Zahlen Statt; denn es sind die oben mit Ψ bezeichneten complexen Zahlen ebenso die Reagentien für die idealen Primfactoren, und die reale Primzahl q, welche nach der Multiplication mit einer solchen als Factor aus dem Producte heraustritt, ist genau Dasselbe, wie der unlösliche Niederschlag, der nach Anwendung des Reagens zu Boden fällt. Auch der Begriff der Äquivalenz ist in der Chemie fast derselbe, wie in der Theorie der complexen Zahlen. So wie nämlich dort zwei Gewichtsmengen verschiedener Stoffe äquivalent heifsen, wenn sie sich gegenseitig vertreten können, entweder zum Zwecke des Neutralisirens, oder um Isomorphie hervorzubringen: so sind zwei ideale Zahlen äquivalent, wenn sie für den Zweck, eine andere ideale Zahl zu einer wirklichen zu machen, sich gegenseitig vertreten können. — Diese hier angedeuteten Analogieen sind nicht etwa als blofse Spiele des Witzes zu betrachten, sondern haben ihren guten Grund darin, dafs die Chemie, so wie der hier behandelte Theil der Zahlentheorie, beide denselben Grundbegriff, nämlich den der ***Zusammensetzung***, wenn gleich innerhalb verschiedener Sphären des Seins, zu ihrem Principe haben; woraus folgt, dafs auch die diesem verwandten, mit ihm nothwendig gegebenen Begriffe sich in beiden auf ähnliche Weise finden müssen. Die Chemie der natürlichen Stoffe und die hier behandelte Chemie der complexen Zahlen sind beide als Verwirklichungen des Begriffs der Zusammensetzung und der davon abhängigen Begriffs-Sphäre anzusehen: jene

Remark

Those who are familiar with the techniques of the development of the theory of algebraic numbers by Kronecker and Dedekind, the successors to Kummer, will find these metaphors foreign to their own experience. Kummer's methods were different, less abstract, with a more immediate appeal. The abstract methods have by now screened the concrete, and the student is often misled. Hermann Weyl, for example, in his notes on algebraic number theory, notes I have already praised, observes after developing the abstract theory and as he is about to apply it to cyclotomic fields, the fields for which Kummer had developed his theory,

> *It is the common curse of all general and abstract theories that they have to be far advanced before yielding useful results in concrete problems.*

I was persuaded by these lines when I first read them four decades ago, and it was not until undertaking these lectures that I appreciated the fallacy in them. There is a great deal to be said for the right abstract, general theories in mathematics and every reason to be impatient with the dull-witted who deny their value simply because they do not understand them, along the lines of the German expression,

> *Was der Bauer nicht kennt, das frißt er auch nicht.*

None the less for the particular concrete problem that Weyl was about to consider, namely cyclotomic fields, the general and abstract theories are not necessary. It is far better and far more instructive to follow Kummer and to deal with the cyclotomic fields directly without any general tools.

The tension between the abstract and the concrete in mathematics has no final resolution, either aesthetically or practically.

so that both[3]

$$\frac{1-\alpha^r}{1-\alpha}$$

and its reciprocal are in $\mathbf{Z}(\alpha)$. Thus it is a unit.

If $n = 3$, then all we have is

$$\frac{1-\alpha^2}{1-\alpha} = 1 + \alpha = -\alpha^2,$$

so that we do not have many units of this form. Otherwise there are many. If $n = 5$, then

$$\alpha \cdot \frac{1-\alpha^4}{1-\alpha} = \alpha(1 + \alpha + \alpha^2 + \alpha^3) = \alpha + \alpha^2 + \alpha^3 + \alpha^4 = -1,$$

so that

$$\frac{1-\alpha^4}{1-\alpha} = -\alpha^4$$

is not of much interest. On the other hand,

$$\alpha^2 \cdot \frac{1-\alpha^2}{1-\alpha} = \alpha^2(1 + \alpha) = \alpha^2 + \alpha^3 = -1 - \alpha^1 - \alpha^4$$

is $1 - w$ if $w = \alpha + \alpha^4$ which is the number $(-1 + \sqrt{5})/2$ we met when treating the regular hexagon. Thus $1 - w$ is $(3 - \sqrt{5})/2$ and

$$\frac{3-\sqrt{5}}{2}\frac{3+\sqrt{5}}{2} = \frac{9-5}{4} = 1$$

is in fact a unit in the domain formed from the square root of 5. If we square $1 - w$, we obtain

$$\frac{9+5-6\sqrt{5}}{4} = \frac{7-3\sqrt{5}}{2}$$

Cubing we obtain

$$\frac{7-3\sqrt{5}}{2}\frac{3-\sqrt{5}}{2} = \frac{36-16\sqrt{5}}{4} = 9 - 4\sqrt{5}.$$

Thus we obtain a solution of Pell's equation,

$$1 + 5x^2 = y^2, \qquad x = 4, \quad y = 9.$$

In a letter to Kronecker dated April 2, 1847 Kummer described how he could prove Fermat's theorem if he made two assumptions, one on the number of classes and one on the units. These assumptions are not always satisfied, so that he was not to obtain in this way a general proof of Fermat's theorem, but he would in the course of years, verify that they were satisfied in many cases, and would in addition show that weaker hypotheses sufficed. Kummer denotes n by λ, but I keep to our notation.

(I) *If a unit has the form $c + n\xi$, where c is an ordinary whole number and ξ is in $\mathbf{Z}(\alpha)$, then it is the nth power of another unit.*

(II) *If $\mathfrak{a}$ is any ideal number then the ideal number $\mathfrak{a}^n$ is the ideal number associated to a number in $\mathbf{Z}(\alpha)$ only if this is already true for $\mathfrak{a}$ itself, or better, as it is stronger, the number of classes of ideal numbers is not a multiple of n.*

[3]Editorial comment: This continues the discussion on p. 298.

If $n = 3$, then there are six units, of which two, ± 1 are certainly third powers, and of which the other four, $\pm\alpha$ and $\pm\alpha^2 = \mp(1+\alpha)$ are not of the form envisaged in the first hypothesis. They are also not third powers. If $n = 2$, then $\mathbf{Z}(\alpha)$ is just the domain $\mathbf{Z}$ of whole numbers but -1 is not a square. So the first hypothesis is not satisfied in this case. For $n = 2$ and $n = 3$, there is a single class. So the number of classes is 1 which is not divisible by n. As we shall see, the proof uses, however, the additional assumption $n > 2$. The stronger form of the second hypothesis is what is usually proved.

I do not want to offer here all of the proof given by Kummer in his letter to Kronecker that Fermat's theorem follows from these two hypotheses. Let me present none the less one of the main ideas. He supposes that

$$x^n + y^n = z^n, \qquad xyz \neq 0 \tag{C}$$

and shows that one of the three numbers x, y or z is necessarily divisible by n, just as we did for $n = 3$. Now we saw for $n = 3$ that n was a unit times $(1-\alpha)^{n-1}$. This is so in general because

$$(1-\alpha)^{n-1} = n\frac{1-\alpha}{1-\alpha}\frac{1-\alpha}{1-\alpha^2}\frac{1-\alpha}{1-\alpha^3}\cdots\frac{1-\alpha}{1-\alpha^{n-1}},$$

as we see on substituting $x = 1$ in the relation

$$(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{n-1}) = x^{n-1} + x^{n-2} + \cdots + x + 1.$$

Thus, as we take n odd, (C) implies a relation

$$u^n - v^n = E(1-\alpha)^{mn}w^n, \qquad m > 0, \quad uvw \neq 0 \tag{D}$$

with E a unit. He shows that such a relation cannot be satisfied even with numbers u, v and w in $\mathbf{Z}(\alpha)$, at least not with numbers satisfying

$$u = c + (1-\alpha)^{mn-n+1}\Phi, \quad v = c + (1-\alpha)^{mn-n+1}\Psi, \tag{E}$$

where Φ and Ψ are in $\mathbf{Z}(\alpha)$ and c is an ordinary whole number. Just as for $n = 3$, there are two steps. It has to be shown that (D) is impossible for $m = 1$. Then it has to be shown that if it is possible for $m > 1$ then it is possible with m replaced by $m - 1$. I consider only the second step, as this makes clear the role of the second hypothesis and the hypothesis $n > 2$.

We can factor $u^n - v^n$ as

$$u^n - v^n = (u-v)(u-\alpha v)(u-\alpha^2 v)\cdots(u-\alpha^{n-1}v). \tag{F}$$

To see this divide both sides by v^n to obtain with $x = u/v$

$$x^n - 1 = (x-1)(x-\alpha)\cdots(x-\alpha^{n-1}).$$

This relation just expresses the fact that

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$$

are all the roots of $x^n - 1 = 0$.

Now we factor (F) into ideal prime factors and use the second hypothesis and the relation (D). Just as for $n = 3$, we see that the factors appearing on the right side of (F) have at most the prime factor associated to $1 - \alpha$ in common. This number does indeed determine a prime ideal. That is easily verified as its norm is n. It is the number we denoted λ for $n = 3$. That means again that one of the numbers on the right side of (F) is divisible by $(1-\alpha)^{mn-n+1}$ and by no higher power, the others being exactly divisible by $1 - \alpha$. All of this is exactly the same as

for $n = 3$. Once again, we can replace u by $\alpha^k u$ with any k as $\alpha^n = 1$. Making use of such a replacement, we may suppose that it is $u - v$ that is exactly divisible by $(1-\alpha)^{mn-n+1}$. This we did for $n = 3$ as well. Thus we have

$$u - v = e(1-\alpha)^{mn-n+1} w_1^n,$$

where at first ew_1^n is only the nth power of an ideal number $\mathfrak{w}$. But the second hypothesis asserts that if the nth power of an ideal number is the ideal number associated to an ordinary number, then that is true of the original ideal number. Consequently $\mathfrak{w}$ is associated to w_1 and the equation (F), in which e is a unit, results.

For similar reasons we have

$$u - \alpha^r v = e_r(1-\alpha^r)t_r^n, \qquad r = 1, \ldots, n-1$$

in which e_r is again a unit.

Kummer has then to make use of the condition (E) and the first hypothesis to ensure that each e_r is an nth power, $e_r = f_r^n$, and to replace $e_r t_r^n$ by z_r^n, $z_r = f_r t_r$. Finally he uses two of the equations

$$u - \alpha^r v = (1-\alpha^r) z_r^n, \tag{G}$$

but to have two of them, he needs $n > 2$ for $0 < r < n$. Consider then (G) and

$$u - \alpha^s v = (1-\alpha^s) z_s^n. \tag{H}$$

Multiply the first by $1-\alpha^s$ and the second by $1-\alpha^r$ and subtract. On the left we obtain

$$\begin{aligned}(1-\alpha^s)(u-\alpha^r v) - (1-\alpha^r)(u-\alpha^s v) &= (\alpha^r - \alpha^s)(u-v) \\ &= (\alpha^r - \alpha^s) e (1-\alpha)^{mn-n+1} w_1^n,\end{aligned} \tag{I}$$

and on the right

$$(1-\alpha^r)(1-\alpha^s)(u_1^n - v_1^n), \tag{J}$$

where, following Kummer, we have set $z_r = u_1$ and $z_s = v_1$.

We want to deduce from the equality of (I) and (J) a relation of the form (D), with u_1, v_1 and w_1 replacing u, v and w and with m replaced by $m-1$. What (I) and (J) give is a relation

$$u_1^n - v_1^n = \frac{(\alpha^r - \alpha^s)(1-\alpha)}{(1-\alpha^r)(1-\alpha^s)} e (1-\alpha)^{mn-n+1} w_1^n. \tag{K}$$

If

$$\frac{(\alpha^r - \alpha^s)(1-\alpha)}{(1-\alpha^r)(1-\alpha^s)} \tag{L}$$

erscheint allerdings günstiger für wissenschaftliche Studien, aber Geldgeschäfte schließen dieselben auch nicht aus. Ich selbst habe in diesem Jahre vielleicht noch weniger mathematisch gearbeitet als Sie. Ich habe nämlich noch keinen neuen Stoff gefunden, und um doch etwas zu thun, werde ich eine Recension über die von JACOBI herausgegebenen dem Könige dedicirten Abhandlungen schreiben. ... — Ich hoffte immer Sie in kurzem einmal hier zu sehen, denn ich denke, die Geschäfte müssen Sie bald einmal herführen, sollten diese es nicht thun, so thun Sie es doch selbst recht bald. Die besten Grüße von den Meinen an Sie und die Ihrigen Ihr Sie herzlich liebender

E. KUMMER.

Breslau, d. 2. April 1847.

Herzlich geliebter Freund!

Versetzen Sie sich wieder einmal in die complexen Zahlen und Einheiten, wo λ, α, u. s. w. lauter bekannte Zeichen sind. Nehmen Sie auch vorläufig einmal folgenden Satz als bewiesen an:

I. „Wenn eine Einheit $E(\alpha)$ die Form hat $E(\alpha) = c + \lambda f(\alpha)$, ($c$ reale g. Z.), so ist $E(\alpha)$ eine λ^{te} Potenz einer andern Einheit."

Der umgekehrte Satz versteht sich ganz von selbst, aber auch dieser ist für $\lambda = 5$ und $\lambda = 7$ sehr leicht zu beweisen, und so überall wo man die Fundamental-Einheiten kennt. Einen allgemeinen Beweis habe ich bisher noch nicht.

II. Es sei ferner λ eine solche Primzahl, für welche die Anzahl aller nicht äquivalenten Formen (oder nach meiner Auffassung der nicht äquivalenten idealen complexen Zahlen) nicht durch λ selbst theilbar ist. Dieß gilt offenbar wieder für $\lambda = 5$, $\lambda = 7$, und für unendlich viele Primzahlen λ, ich weiß nicht ob für alle. Es wird unter dieser Voraussetzung, wenn $(f(\alpha))^\lambda$ eine wirkliche complexe Zahl ist, allemal auch $f(\alpha)$ selbst eine wirkliche complexe Zahl sein; denn die Potenz, welche die ideale Zahl zur wirklichen macht, hat stets mit der Anzahl der nicht äquivalenten Formen einen gemeinschaftlichen Factor.

Für alle diejenigen Primzahlen λ, welche diesen beiden Bedingungen I und II genügen kann ich nun die Unmöglichkeit der Gleichung $x^\lambda - y^\lambda = z^\lambda$ vollständig beweisen wie folgt.

Zunächst beweise ich, daß wenn $x^\lambda - y^\lambda = z^\lambda$ Statt haben soll, eine der drei Zahlen durch λ theilbar sein muß. Sei x nicht durch λ theilbar, so giebt $x^\lambda = z^\lambda + y^\lambda$ folgende Gleichungen:

$$z + y = a^\lambda \quad \text{und} \quad z + \alpha^r y = E(\alpha) f(\alpha)^\lambda$$

ich verwandle α in α^{-1}, wodurch

$$z + \alpha^{-r} y = E(\alpha^{-1}) f(\alpha^{-1})^\lambda$$

es ist aber

$$E(\alpha^{-1}) = \pm \alpha^x E(\alpha), \quad \text{also} \quad z + \alpha^{-r} y = \pm \alpha^x E(\alpha) f(\alpha^{-1})^\lambda$$

also wenn $E(\alpha)$ eliminirt wird

$$\pm \alpha^x (z + \alpha^r y) f(\alpha^{-1})^\lambda = (z + \alpha^{-r} y) f(\alpha)^\lambda.$$

Hieraus eine Congruenz mod λ gemacht, giebt $f(\alpha)^\lambda \equiv c \mod \lambda$, ebenso $f(\alpha^{-1}) \equiv c \mod \lambda$ also, weil c nicht durch λ theilbar ist,

$$\pm \alpha^x (z + \alpha^r y) \equiv z + \alpha^{-r} y \mod \lambda$$

oder

$$0 \equiv z + \alpha^{-r} y \mp \alpha^x z \mp \alpha^{x+r} y \mod \lambda.$$

Diese Congruenz kann nicht bestehen, ohne daß eine der Zahlen z oder y durch λ theilbar ist. q. e. d. Es sei also z die durch λ theilbare Zahl.

Anstatt der Gleichung $x^\lambda - y^\lambda = z^\lambda$, wo z durch λ theilbar ist, behandle ich die allgemeinere Gleichung für complexe Zahlen:

1) $$u^\lambda - v^\lambda = E(\alpha)(1-\alpha)^{m\lambda} w^\lambda \quad (E(\alpha) \text{ Einheit})$$

wo u, v, w complexe Zahlen sind, w den Factor $1-\alpha$ nicht weiter enthaltend, und ich setze von u und v nur das voraus, daß sie in folgende Form gebracht werden können:

2) $$u = c + (1-\alpha)^{m\lambda - \lambda + 1} \cdot \Phi(\alpha); \quad v = c + (1-\alpha)^{m\lambda - \lambda + 1} \cdot \Psi(\alpha). \quad (c \text{ real}).$$

Ich zerlege nun $u^\lambda - v^\lambda$ in seine λ complexen Factoren, $u - v$, $u - \alpha v$, $u - \alpha^2 v$, etc. Diese Factoren haben unter sich keinen gemeinschaftlichen Factor außer $1-\alpha$, diesen aber haben sie alle und zwar jedes nur einmal, eins aber hat ihn alle übrigen male, und dieß ist nach der Voraussetzung (siehe 2) $u - v$ es ist also

3) $$u - v = e(\alpha)(1-\alpha)^{m\lambda - \lambda + 1} \cdot w_1^\lambda$$

4) $$u - \alpha^r v = e_r(\alpha)(1-\alpha^r) t_r^\lambda$$

$e(\alpha)$ und $e_r(\alpha)$ sind Einheiten, w_1 und t_r complexe Zahlen.

(Der Satz: „wenn eine Potenz einer complexen Zahl in Factoren zerlegt wird, welche relative Primzahlen sind, so müssen diese Factoren

selbst ebensolche Potenzen sein, multiplicirt mit Einheiten", folgt klar aus meinen früheren Untersuchungen, noch ist zu bemerken, daß weil w_1^λ und t_r^λ wirkliche complexe Zahlen sind, auch w_1 und t_r selbst solche sein müssen, nach der obigen Voraussetzung.)

Ich substituire in 4) die Werthe des u und v aus 2), so wird, wenn durch $1-\alpha^r$ dividirt ist:

$$5) \qquad c + (1-\alpha)^{m\lambda-\lambda} \cdot \left(\frac{1-\alpha}{1-\alpha^r}\right)(\Phi(\alpha) - \alpha^r \Psi(\alpha)) = e_r(\alpha)\, t_r^\lambda$$

Hieraus mache ich eine Congruenz modulo λ und bemerke, daß $(1-\alpha)^{m\lambda-\lambda}$ durch λ theilbar ist, wenn $m > 1$, welches hier vorausgesetzt wird, so ist

$$c \equiv e_r(\alpha)\, t_r^\lambda \mod \lambda;$$

es ist aber die λ^{te} Potenz der complexen Zahl allemal einer realen Zahl congruent, also $t_r^\lambda \equiv b \mod \lambda$ folglich

$$c \equiv e_r(\alpha) b \mod \lambda,$$

und weil $e_r(\alpha)$ einer realen Zahl congruent ist modulo λ, so ist, nach dem oben angenommenen Satze, $e_r(\alpha)$ gleich einer λ^{ten} Potenz einer andern Einheit, also $e_r(\alpha) t_r^\lambda$ gleich einer λ^{ten} Potenz, gleich u_1^λ.

Dieß in der Gleichung (4) substituirt, giebt

$$6) \qquad u - \alpha^r v = (1-\alpha^r) u_1^\lambda$$

ebenso hat man für irgend einen anderen Werth des r, welchen ich s nenne

$$7) \qquad u - \alpha^s v = (1-\alpha^s) v_1^\lambda$$

und wenn noch die Gleichung 3) hinzugenommen wird:

$$3) \qquad u - v = e(\alpha)(1-\alpha)^{m\lambda-\lambda+1} \cdot w_1^\lambda$$

und aus diesen u und v eliminirt werden, so erhält man

$$u_1^\lambda - v_1^\lambda = \frac{(\alpha^r - \alpha^s) e(\alpha)(1-\alpha)^{m\lambda-\lambda+1} \cdot w_1^\lambda}{(1-\alpha^r)(1-\alpha^s)}$$

und wenn

$$\frac{(\alpha^r - \alpha^s)(1-\alpha)}{(1-\alpha^r)(1-\alpha^s)} e(\alpha) = E_1(\alpha)$$

gesetzt wird

$$8) \qquad u_1^\lambda - v_1^\lambda = E_1(\alpha)(1-\alpha)^{(m-1)\lambda} \cdot w_1^\lambda .$$

Diese Gleichung 8) ist nun dieselbe als 1) nur $m-1$ statt m gesetzt. Um aber zu zeigen, daß dieselbe Verwandlung sich wieder mit dieser Gleichung vornehmen läßt, müssen wir auch noch beweisen, daß die

is a unit, then its product with e is again a unit e_1 and the relation (K) becomes

$$u_1^n - v_1^n = e_1(1-\alpha)^{(m-1)n} w_1^n,$$

which is exactly like (D) but with m replaced by $m-1$. Of course the conditions (E) have still to be verified, but that we leave to Kummer.

The expression in (L) is

$$\alpha^r \cdot \frac{1-\alpha^{s-r}}{1-\alpha} \frac{1-\alpha}{1-\alpha^r} \frac{1-\alpha}{1-\alpha^s},$$

thus the product of four expressions, all of which is a unit. So it is a unit.

Kummer was able to verify the two hypotheses for a large number of primes. They are true for all primes less than 100 except 37, 59 and 67, but it is not known that they are true for an infinite number of primes.

We do not have time to discuss Kummer's efforts to verify his hypotheses. Nor do we have time, or perhaps even the inclination, to discuss the methods introduced by Kummer and others to circumvent the difficulties entailed by the lack of general validity of these hypotheses. Kummer's claims to greatness rest as much on his creation of a rich theory of algebraic numbers and on discoveries that remain, even after the resolution of Fermat's theorem, very near mysteries that are at the core of modern number theory as they do on his very bold, highly acclaimed, but ultimately only partially successful treatment of Fermat's theorem. I had hoped initially to offer in these lectures a glimpse of these mysteries to a lay audience and at the same time, by removing them from an abstract, theoretical sphere burdened with definitions to a plane where their significance would be immediately comprehensible, to acquire myself some adequate insight into their meaning. Frankly, in this respect, I have not come very far along, and am still about where I was a year ago. With the first set of lectures behind me, I can perhaps(!) now begin to think about a second in which I try again.

The mysteries to which I refer are to a large extent conjectures about the relation between numbers defined in one way or another by attempts to analyze the solutions of equations in integers or rational numbers and numbers defined by analytic expressions, thus expressions whose formation requires integrals and infinite series, but which can nevertheless, in contrast to the first class of numbers, be—provided various other conjectures can be established—calculated readily. Kummer was one of the first to discover such relations. The number of ideal classes of $\mathbf{Z}(\alpha)$ is a number of the first type. It is by no means clear how to calculate it, yet Kummer, for his purposes, needs to show that it is prime to n. This is his second hypothesis. What he eventually showed is that his two hypotheses are valid if and only if the prime n does not divide the numerator of a certain collection of numbers, called Bernoulli numbers. These numbers can be defined in an elementary way, and I shall do so. Not only can they be readily calculated as we shall see, but also they are, in essence, the value of a very famous function, the Riemann zeta function, at negative integers. This function is defined by summing an infinite series.

There are many relations of this sort presently conjectured. The conjectures are magnificent, and it is a still outstanding task of the modern mathematician not only to prove them but also to explain them to himself and to the rest of the world.

The Bernoulli numbers B_0, B_1, B_2, and so on, can be defined in a simple way. First of all, $B_0 = 1$. Then, in general,[4]

$$B_n = -\frac{1}{n+1}\left(B_0 + (n+1)B_1 + \cdots + \frac{n(n+1)}{2}B_{n-1}\right)$$

Thus

$$B_1 = -\frac{1}{2}B_0 = -\frac{1}{2},$$
$$B_2 = -\frac{1}{3}\left(1 + 3\left(-\frac{1}{2}\right)\right) = \frac{1}{6},$$
$$B_3 = -\frac{1}{4}\left(1 + 4\left(-\frac{1}{2}\right) + 6\left(\frac{1}{6}\right)\right) = 0,$$
$$B_4 = -\frac{1}{5}\left(1 + 5\left(-\frac{1}{2}\right) + 10\left(\frac{1}{6}\right) + 10(0)\right) = -\frac{1}{30}.$$

The numbers grow rapidly, except that B_k, k odd, and $k \neq 1$, is always 0. For example,

$$B_{30} = \frac{8615841276005}{14322}.$$

Kummer's criterion for a prime n to satisfy his two hypotheses is that n does not divide the numerator of the numbers $B_2, B_4, \ldots, B_{n-3}$. For example 5 does not divide the numerator of B_2 which is 1 and 7 does not divide the numerator of B_2 or of B_4, which is 1. Since, for example,

$$B_6 = \frac{691}{2730},$$

the prime 691 will not satisfy Kummer's hypotheses. We also have

$$B_{32} = \frac{7709321041217}{510}$$

and

$$7709321041217 = 37 \times 683 \times 305065927,$$

so that $n = 37$ does not satisfy Kummer's hypotheses.

[4]Editorial comment:

$$B_n = -\frac{1}{n+1}\left(B_0 + (n+1)B_1 + \cdots + \frac{n(n+1)}{2}B_{n-1}\right) = -\frac{1}{n+1}\sum_{k=0}^{n-1}\binom{n+1}{k}B_k.$$

Compiled on May 1, 2026.