

BO1 History of Mathematics
Lecture XV
Geometry and number theory

MT 2019 Week 8

Summary

- ▶ Euclid's *Elements* revisited
- ▶ The parallel postulate
- ▶ Non-Euclidean geometry
- ▶ Number theory down the centuries

Euclid's *Elements*

Euclid's *Elements*, in 13 books, compiled c. 250 BC.

Books I–V: definitions, postulates, plane geometry of lines and circles

Book VI: similarity, proportion

Books VII–IX: number theory

Book X: commensurability, irrational numbers, surds

Books XI–XIII: solid geometry ending with the classification of the regular polyhedra

Euclid's *Elements*

Euclid's *Elements*, in 13 books, compiled c. 250 BC.

Books I–V: definitions, **postulates**, plane geometry of lines and circles

Book VI: similarity, proportion

Books VII–IX: **number theory**

Book X: commensurability, irrational numbers, surds

Books XI–XIII: solid geometry ending with the classification of the regular polyhedra

Euclid in English

BOOK I.

DEFINITIONS.

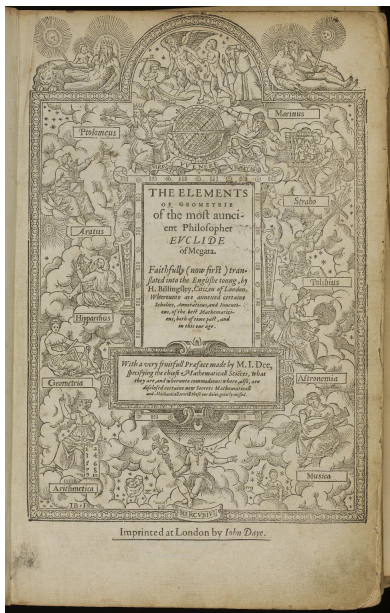
1. A **point** is that which has no part.
2. A **line** is breadthless length.
3. The extremities of a line are points.
4. A **straight line** is a line which lies evenly with the points on itself.
5. A **surface** is that which has length and breadth only.
6. The extremities of a surface are lines.
7. A **plane surface** is a surface which lies evenly with the straight lines on itself.
8. A **plane angle** is the inclination to one another of two lines in a plane which meet one another and do not lie in a straight line.
9. And when the lines containing the angle are straight, the angle is called **rectilinear**.
10. When a straight line set up on a straight line makes the adjacent angles equal to one another, each of the equal angles is **right**, and the straight line standing on the other is called a **perpendicular** to that on which it stands.
11. An **obtuse angle** is an angle greater than a right angle.
12. An **acute angle** is an angle less than a right angle.
13. A **boundary** is that which is an extremity of anything.
14. A **figure** is that which is contained by any boundary or boundaries.
15. A **circle** is a plane figure contained by one line such that all the straight lines falling upon it from one point among those lying within the figure are equal to one another ;



Canonical English edition by
Sir Thomas L. Heath, 1908

See also the [Reading Euclid Project](#)

Billingsley's Euclid, 1570



The Elements of Geometrie:

“Faithfully (now first) translated into the English tongue” by H. Billingsley, London, 1570

[Available online](#)

Preface by John Dee

Dee's Preface

TO THE VNFAINED LOVERS
of truth, and constant Studentes of Noble
Sciences, JOHN DEE of London, hartly
wist heth grace from heaven, and most prosper-
ous success in all their best attempts and
exercyses.

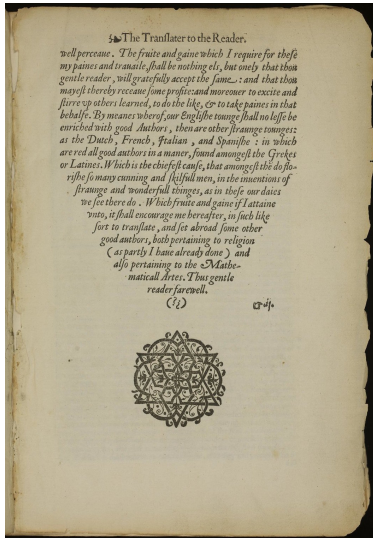
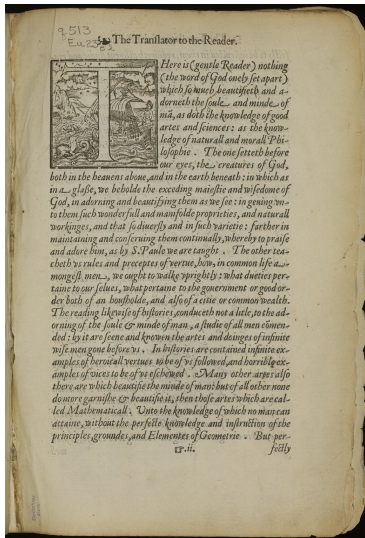


Inaine *Plato*, the great Master
of many worthy Philosophers,
and the constant souch, and
pithy perswader of *Plato*, *Eu-
clid*, and *Aristo*; in his Schole and
Academie, sundry times (besides
his ordinary Scholers) was visited
of a certaine kinde of men, allured
by the noble fame of *Plato*, and
the great commendation of his
profound and profitable doctrine.
But when such Hearers, after long
hearkning to him, perceived that
the drift of his discourses issued
out, to conclud, this *Plato*, *Eu-
clid*, and *Aristo*, to be Spirituall, In-
finite, Aeternall, Omnipotent, &c.

Nothing being alledged or required. How worldly goods, how worldly digni-
ties, how health, strength or luffines of body; nor yet the names, how a mansions
sensible and bodily blisid and felicitie hereafter, might be attained: Seraphicway,
the fantasies of those hearers, were damp; their opinion of *Plato*, was cense chaung-
ed; yea his doctrine was by them despised; and his Schole, no more of them visit-
ed. Which thing his Schole, *Aristo*, narrowly observing, kande the cause thereof,
of, to be, For that they had no forwarning and information, in generall, whereto
his doctrine tended. For, in might they have had occasion, either to have forborne
his Schole haunting; (if they, them, had mist of his Scope and purpose) or constan-
tly to have continued therein to their full satisfaction: if that his small scope be
intent, had ben to their desire. Wherfore, *Aristo*, ever, after that, yed in lict, to
forewarne his owne Scholers and hearers, both of what matter, and also to what
code, he stoke in hand to speake, or teach. While I consider the diuine trades of
these two excellent Philosophers (and am much more, both, when *Plato* might well, as
therwise could teach: and that, *Aristo*, might boldly, with his hearers, have
dealt in like sort as *Plato* did) I am in no little pang of perplexitie: Bycause, that,
which I unlik, is most easy for me to performe (and to haue *Plato* for my exaple.)
And that, which I know to be most commendable: and (in this first bringing, into
common handling, the *Arts*, & *Mathematices*) to be most necessary: is full of great
difficultie and sundry daungers. Yet, neither do I think it meet, for io strange mat-
ters (as now is ment to be published) and to so strange an audience, to be blantly,
at first, put forth, without a peculiar Preface: Nor (imiting *Aristo*) will can I
hope, that according to the ample and dignitie of the *Arts*, & *Mathematices*, I
am able, either playly to prescribe the materiall boundes: or precisely to expresse
the chief purposes, and most wonderful applications thereof. And though I am
sure, that such as did thinke from *Plato* his Schole, after they had perceived his fi-
nite



Billingsley's Preface, pp. 1, 3



Pop-up Euclid

will narrow or enlarge, as length ends the it angles (or the length or width thereof), in one point. So all their angles shew beyond together make a solid angle. And for the better light shewed, I have here drawn a figure whereby to build more easily conceive, the base of the figure is a triangle, *A B C*, of an every side of the triangle *A B C* extend up a straight line from the side *A B*, or rather up the straight line *A B* from the side *A C*, the straight line *A C*, and from the side *B C*, the straight line *B C*, and to bring the straight lines up, that their upper ends, the points *F* above and lower together in one point, so that they plainly shew how these superficiesall angles *A B F*, *B C F*, *A C F* are made, and close together, touching the one the other in the point *F*, and so make a solid angle.



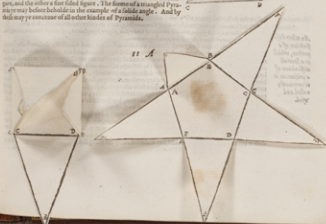
11 A Pyramid is a solide figure contained under many plaine superficieses set upon one plaine superficies, and gathered together in one point.

Teach definition.

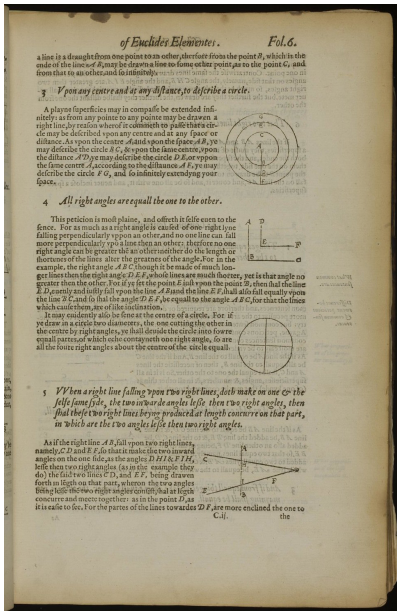
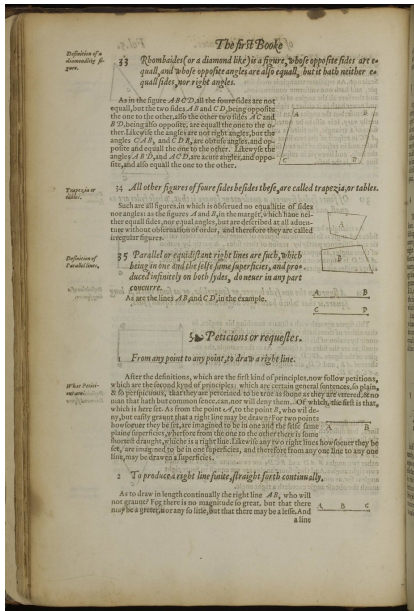
Two superficieses raised upon any ground can not make a Pyramid, for that two superficieses raised together in the top, cannot, as before is shewd, make a solid angle. Wherby what the square, the circle, or any other figure is raised upon, is not a pyramid, but a solid angle. Wherby what the square, the circle, or any other figure is raised upon, is not a pyramid, but a solid angle. Wherby what the square, the circle, or any other figure is raised upon, is not a pyramid, but a solid angle.

And because that all the superficieses of every Pyramid is raised from one plaine superficieses from the base and made in one point, or more convenient to say, that all the superficieses of a Pyramid are triangular, except the base, which may be of any forme or figure except a circle. For if the base be a circle, then it is not a pyramid, but a solid angle, or more convenient to say, that all the superficieses of a Pyramid are triangular, except the base, which may be of any forme or figure except a circle.

Of Pyramids, there are divers kinds. For according to the variety of the base, there is called a triangular Pyramid, a quadrangular Pyramid, a pentagonal Pyramid, and so forth according to the variety of the angles of the base indifferently. Although the figure of a Pyramid can not be well expressed in a plaine superficieses, yet may it sufficiently conceive of it both by the figure before set in the solution of a solid angle, and by the figure here set, if you imagine the point *A* together with the lines *A B*, *A C*, and *A D*, to be closed up high. And yet that the reader may more clearly see the forme of a Pyramid, I have here set two handy Pyramids which will appear to be the same, if you consider the papers wherin are drawn on the triangular sides of the Pyramid, in such sort that the corners of the angles of each triangle may in every Pyramid concur in one point, and make a solid angle: one of which hath for his base a four sided figure, and the other a five sided figure. The forme of a triangular Pyramid may be better beheld in the example of a solid angle. And by this may it conceive of all other kinds of Pyramids.

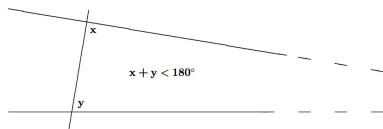
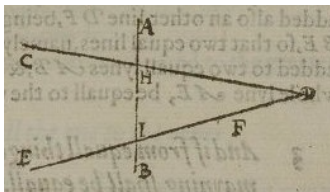


Book I: postulates



Postulate 5

5 When a right line falling vpon two right lines, doth make on one & the selfe same syde, the two inwarde angles lesse then two right angles, then shal these two right lines beyng produced at length concurre on that part, in which are the two angles lesse then two right angles.



Equivalent formulation (Proclus, 5th century; John Playfair, 1795):
given a straight line L and a point P not on L there is one and only one straight line through P that is parallel to L .

Classical disquiet about the fifth postulate

Original to Euclid? Less 'self-evident' than the other postulates?

Euclid used it (e.g., in the proof of Proposition 29 of Book I), so the property is necessary — but does it in fact follow from the other postulates?

Proclus in commentary on Euclid, 5th century (after citing Ptolemy's attempted proof of the parallel postulate, and discussing the nature of truth, with reference to Aristotle and Plato):

It is then clear from this that we must seek a proof of the present theorem, and that it is alien to the special character of postulates.

Attempted (unsuccessfully) to prove the fifth postulate on the basis of the others

See Heath, pp. 202–220

Mediaeval disquiet about the fifth postulate

In the Islamic world:

Ibn al-Haytham (Alhazen) (965–1039) attempted (unsuccessfully) to prove the parallel postulate by contradiction

Omar Khayyám (1050–1123) attempted to prove the fifth postulate on the basis of the following alternative:

two convergent straight lines intersect and it is impossible for two convergent straight lines to diverge in the direction in which they converge

Described the situations that may occur if the postulate is **omitted**

Nasir al-Din al-Tusi (1201–1274) criticised Khayyám's attempted proof, offered his own

Al-Tusi's thoughts found their way into Europe via the writings (1298) of his son Sadr al-Tusi

Early modern disquiet about the fifth postulate

After reading al-Tusi, John Wallis showed that the parallel postulate is equivalent to the following:

on a given finite straight line it is always possible to construct a triangle similar to a given triangle

He lectured on this in Oxford in 1663

Attempts to prove the fifth postulate on the basis of Euclid's other axioms had resulted only in equivalent forms — so can we have a consistent geometry in which the parallel postulate **fails**?

Early hints of non-Euclidean geometry

Giovanni Girolamo Saccheri (1667–1733): sought to establish the validity of Euclidean geometry — negated the parallel postulate in search of a contradiction; two cases:

- ▶ internal angles of a triangle add up to less than two right angles — contradicts Euclid's second postulate
- ▶ internal angles of a triangle add up to more than two right angles — leads to non-intuitive ideas

Similar results derived by Johann Heinrich Lambert (1728–1777) in his *Theorie der Parallelinien* (1766)

Non-Euclidean geometries

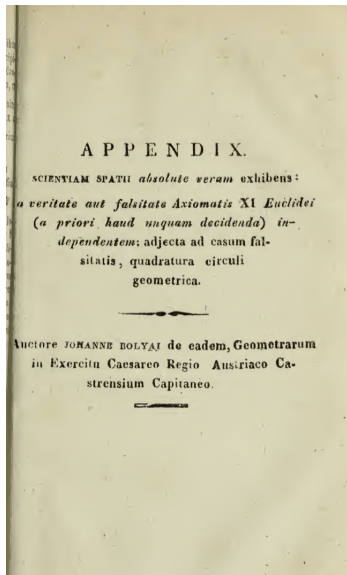
Consistent non-Euclidean geometry probably first constructed (tentatively) by Gauss, c. 1817–1830, but remained unpublished

Problem pursued independently (without success) by Gauss' friend Farkas Bolyai (1775–1856)



Pursued (against paternal advice) and solved by János Bolyai (1802–1860): “I have created a new and different world out of nothing” (1823)

Bolyai's geometry



Published as appendix 'The science absolute of space: independent of the truth or falsity of Euclid's axiom XI (which can never be decided a priori)' to father's textbook

Tentamen iuventutem studiosam in elementa matheosos introducendi (1832)

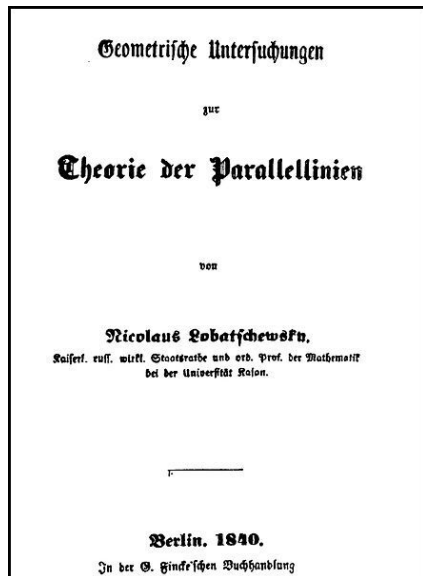
English translation by George Bruce Halstead (1896)

Meanwhile in Russia...



Non-Euclidean geometry developed independently by Nikolai Ivanovich Lobachevskii [Николай Иванович Лобачевский] (1792–1856) using the negation of Playfair's axiom

Lobachevskii's works



Complicated story of dissemination...

Geometriya [Геометрия] written in 1823 but was not published until 1909

Ideas presented in Kazan in 1826, published there 1829 — but rejected by St Petersburg Academy (a translation of the review is available [here](#))

Other works in Russian, French and German, including *Geometrische Untersuchungen zur Theorie der Parallellinien* (1840), *Pangéométrie* (1855)

Acceptance and impact of non-Euclidean geometries

Slow to gain acceptance due to

- ▶ obscurity of publications
- ▶ lack of intuitive understanding

But non-Euclidean geometries

- ▶ overturned old ideas of mathematical certainty
- ▶ introduced new ideas about space
- ▶ helped drive the late 19th-century move towards axiomatisation

The Euclidean algorithm (Proposition VII.2)

The seventh Book

multiple number B A, wherefore it also measurith this which remaineth next, the number F A (by the 5. common fence of the seventh). But the number A F measurith the number D G wherefore A also measurith D G. And it measurith also the whole D C, wherefore it also measurith the number F B, wherefore also E measurith F H, and it measurith the whole number F A, wherefore (by the first common fence) it also measurith that which remaineth H A, which is to witte, it self being a number, which is impossible. Wherefore no prime number doth measure the numbers A B and C D, wherefore the numbers A B and C D are prime numbers the one to the other: which was required to be proved.

The converse of this proposition after Campanus.

And if the two numbers, namely A B and C D be prime to the other, then the life being continually taken from the greater there be left before you come to unity. For if in the continual subtraction there be left before you come to unity. Suppose that H A be the number wherein the life is made, which also being divided out of G C cleaveth nothing. Wherefore H A measurith G C where also it measurith H B by the 5. common fence of the fourth. And the residue of the fourth is H C, therefore it also measurith the whole A B, by the first common fence of the fourth. And it measurith also the whole number A B by the first common fence of the fourth. And it measurith also the whole number A B by the first common fence of the fourth. Now how far so much as the number H A measurith the numbers A B and C D, therefore the numbers A B and C D are numbers compounded wherefore they are not prime to the other: which is contrary to the hypothesis.

And by this proposition if there be two numbers given, it is easy to finde out whether they be prime the one to the other or no. For if by each continual subtraction of the little from the greater, you come at length to unity, then are those numbers given prime the one to the other. But if there be a life before you come to unity, then are the numbers given numbers compounded the one to the other.

The 1. Probleme. The 2. Proposition.

Two numbers being given not prime the one to the other, to finde out their greatest common measure.

Propose the two numbers given not prime the one to the other to be A B and C D. It is required to finde out the greatest common measure of the said numbers. Let A B and C D. Now if C D either measurith the number A B or not. If C D measurith A B it shall be A B where it self. Wherefore C D is a common measure of the numbers A B C D and A B. And it is manifestly evident that it is the greatest common measure, for there is no number greater then C D that may measure C D.

But if C D do not measure A B, then if of the numbers A B B and C D, the life be continually taken away from the greater, C D there will before you come to unity, the life a number, which will measure the number given before you (by the 5. fence of the seventh). For if there be left out the number A B and C D, the residue of the one to the other which is contrary to the hypothesis. Let the said number left before you continually subtraction of the little number out of the greater be E C. So that let the number C D be subtracted out of it as often as you can leave a life number: then it self, namely A E. And let A E measure C D, and subtracted out of it

Two cases in this proposition. The first case. The second case.

of Euclides Elementes Fol. 189.

as often as you can leave a life there is left a number, C E. And suppose that C E do measure A E. that there remaineth nothing. Then I say that C E is a common measure to the number A B and C D. For first of all as C E measurith A E, and A E measurith D F, therefore C E also measurith D F (by the fifth common fence of the seventh) and it likewise measurith F B, wherefore it also measurith the whole C D (by the sixth common fence of the seventh) but C E measurith B E, wherefore C E also measurith B E (by the fifth common fence of the seventh). And it measurith also A E, wherefore it also measurith the whole B A (by the sixth common fence of the seventh) and it also measurith C D as we have before proved: wherefore the number C E measurith the numbers A B and C D, wherefore the number C E is a common measure to the numbers A B and C D.

Demons-tration of the second case. That C E is a common measure to the numbers A B and C D.

If any other that is the greatest common measure. For if C E be not the greatest common measure to A B and C D, let there be a number greater then C E which measurith A B and C D, which let be G. And A B first of all as G measurith C D, and C D measurith B E, G D therefore G also measurith B E (by the fifth common fence of the seventh) and it measurith the whole A B, wherefore also it measurith the residue, namely, A E (by the 5. common fence of the seventh). But A E measurith D F, wherefore G also measurith D F (by the first of all, common fence of the seventh) And it measurith the whole C D. Wherefore it also measurith the residue F C, namely, the greater number the life, which is impossible. No number therefore greater then C E shall measure their numbers A B and C D, wherefore C E is the greatest common measure to A B and C D, which was required to be done.

Corollary.

Hereby it is manifest, that if a number measure two numbers it shall also measure their greatest common measure. For if it measure the whole & the part taken away it shall always measure the residue also, which residue is of the length, the greatest common measure of the two numbers given.

The 2. Probleme. The 3. Proposition.

Three numbers being given not prime the one to the other: to finde out their greatest common measure.

Propose the three numbers given not prime the one to the other to be A B, C. Now it is required to finde out the said numbers A B C D. Now I say that to finde out the greatest common measure, I take the greatest common measure of the two numbers A and B (by the 2. of the seventh) which let be D: which number D either measurith the number C or not.

Two cases in this Proposition. The first case.

First let D measure C. And it also measurith the numbers A B, and wherefore D measurith the numbers A B, C. Wherefore D is a common measure unto the numbers A B, C. Now I say also that it is the greatest common measure unto them. For if D be not the greatest common measure of the two numbers A, B, C, let some number greater then D measure the numbers A, B, C. And let the same number be E. Now first of all as E measurith the numbers A, B, C, it measurith also the numbers A, B. Wherefore it measurith also

the number C, which is contrary to the hypothesis.

Euclid on prime numbers (Proposition IX.20)

of Euclides Elementer. Fol. 212.

But now suppose that A do not measure D . Then I say that it is not possible to finde out a fourth number proportionall with these numbers A, B, C . For if it be possible, let there be found such a number, and let the same be E . Wherefore that which is produced of C into E is equal to that which is produced of B into C . But that which is produced of B into C is D . Wherefore that which is produced of A into E is equal to D . Wherefore A multiplieth E produced D , wherefore A mesureth D , but it also mesureth it not, which is impossible. Wherefore it is impossible to finde out a fourth number proportionall, with these numbers A, B, C , whensoever A mesureth not D .

But now suppose that A, B, C be together in continual proportiō, neither all in these extremes be prime the one to the other. And let B mult

A
B
C
E
D 1350

tiplicyng C produce D . And in like sorte may we prove that if A do measure D , it is possible to finde out a fourth number proportionall with them. But if it do not measure D , this is it possible: which was required to be proved.

¶ The 20. Theorem. The 20. Proposition.

Prime numbers being geuen how many soeuer, there may be geuen a prime number.

Suppose that the prime numbers geuen be A, B, C . Then I say, that there yet more prime numbers besides A, B, C . Take (by the 38. of the seventh) the least number whom these numbers A, B, C do measure, and let the same be D . And vnto $D E$ adde vntill $D F$. Now $E F$ is either a prime number or First let it be a prime number, then are there found these prime numbers A, B, C , and $E F$ more in multitude then the prime numbers first geuen A, B, C . But now suppose that $E F$ be not prime. Wherefore some prime number mesureth it (by the 24. of the seventh). Let a prime number measure it, namely, G . Then I say, that G is none of these numbers A, B, C . For if G be one and the same with any of these A, B, C . But A, B, C measure the number $D E$: wherefore G also mesureth $D E$: and it also mesureth the whole $E F$. Wherefore G being a number shall measure the residue $D F$ being vntill: which is impossible. Wherefore G is not one and the same with any of these prime numbers A, B, C : and it is also supposed to be a prime number. Wherefore there are found these prime numbers A, B, C, G , being more in multitude then the prime numbers geuen A, B, C : which was required to be demonstrated.

* A Corollary.

By this Proposition it is manifest, that the multitude of prime numbers is infinite.

¶ The 21. Theorem. The 21. Proposition.

If euen numbers how many soeuer be added together: the whole shall be euē.

E.E.ij. Suppos

Prime numbers being geuen how many soeuer, there may be geuen more prime numbers.



Suppose that the prime numbers geuen be A, B, C . Then I say, that there are yet more prime numbers besides A, B, C . Take (by the 38. of the seventh) the least number whom these numbers A, B, C do measure, and let the same be $D E$. And vnto $D E$ adde vntill $D F$. Now $E F$ is either a prime number or not.

First let it be a prime number, then are there found these prime numbers A, B, C , and $E F$ more in multitude then the prime numbers first geuen A, B, C .

But now suppose that $E F$ be not prime. Wherefore some prime number mesureth it (by the 24. of the seventh). Let a prime number measure it, namely, G . Then I say, that G is none of these numbers A, B, C . For if G be one and the same with any of these A, B, C . But A, B, C measure the number $D E$: wherefore G also mesureth $D E$: and it also mesureth the whole $E F$. Wherefore G being a number shall measure the residue $D F$ being vntill: which is impossible. Wherefore G is not one and the same with any of these prime numbers A, B, C : and it is also supposed to be a prime number. Wherefore there are found these prime numbers A, B, C, G , being more in multitude then the prime numbers geuen A, B, C : which was required to be demonstrated.

A ..
B ...
C
E 114
D . F
G

Euclid on perfect numbers

is double to 3; and to 4 double to 3. Likewise these four numbers are in like proportion 9:6 as 6:4 for what partes of each part is called 2: 3 of 6 is a third part, to 4 also is of 6 a third part: So are these four numbers also in proportion 4:3 as 3:2: what partes are of such partes are of 2: 1 of 3 are two third partes, likewise of 4 are two third partes. Moreover, these numbers are in 3: 2 as in proportion for what are these many partes of each 6: 6 many partes are 1: 1 of 6 is a fourth part, for one third part of 6 is 2, which take four times make 8: 8 is 2 of 3, 1/3 is four third partes: for one third part of 6 is 2, which when foure times make 8: 8 is 2 of 3, 1/3 is four third partes: 1: 1 of 6 is 2, which when foure times make 8: 8 is 2 of 3, 1/3 is four third partes.

23 *A perfect number is that, which is equall to all his partes.*

As the partes of 6 are 1. 2. 3. three is the halfe of 6, two the third part, and 1. the sixth part, and mo partes 6 hath not: which three partes 1. 2. 3. added together, make 6 the whole number, whose partes they are. Wherefore 6 is a perfect number. So likewise is 28 a perfect number, the partes whereof are these numbers 14. 7. 2 and 1: 14 is the halfe therof, 7 is the quarter, 4 is the seventh part, 2 is a fourth part, and 1 an 28 part, and these are all the partes of 28. all which, namely, 1, 2, 4, 7 and 14 added together, make iustly without more or lesse 28. Wherefore 28 is a perfect number, and so of others the like. This kinde of numbers is very rare and seldome found. From 1 to 10, there is but one perfect number, namely, 6. From 10 to an 100, there is also but one, that is, 28. Also from 100 to 1000 there is but one which is 496. From 1000 to 10000 likewise but one. So that betwene every stay in numbring, which is euier in the tenth place, there is found but one perfect number And for their rarenes and great perfection, they are of maruelous vse in magike, and in the secret part of philosophy.

This kinde of numbers called perfect numbers

perfect partes of 6: 1. 2. 3. three is the halfe of 6, two the third part, and 1. the sixth part, and mo partes 6 hath not: which three partes 1. 2. 3. added together, make 6 the whole number, whose partes they are. Wherefore 6 is a perfect number. So likewise is 28 a perfect number, the partes whereof are these numbers 14. 7. 2 and 1: 14 is the halfe therof, 7 is the quarter, 4 is the seventh part, 2 is a fourth part, and 1 an 28 part, and these are all the partes of 28. all which, namely, 1, 2, 4, 7 and 14 added together, make iustly without more or lesse 28. Wherefore 28 is a perfect number, and so of others the like. This kinde of numbers is very rare and seldome found. From 1 to 10, there is but one perfect number, namely, 6. From 10 to an 100, there is also but one, that is, 28. Also from 100 to 1000 there is but one which is 496. From 1000 to 10000 likewise but one. So that betwene every stay in numbring, which is euier in the tenth place, there is found but one perfect number And for their rarenes and great perfection, they are of maruelous vse in magike, and in the secret part of philosophy.

perfect partes of 6: 1. 2. 3. three is the halfe of 6, two the third part, and 1. the sixth part, and mo partes 6 hath not: which three partes 1. 2. 3. added together, make 6 the whole number, whose partes they are. Wherefore 6 is a perfect number. So likewise is 28 a perfect number, the partes whereof are these numbers 14. 7. 2 and 1: 14 is the halfe therof, 7 is the quarter, 4 is the seventh part, 2 is a fourth part, and 1 an 28 part, and these are all the partes of 28. all which, namely, 1, 2, 4, 7 and 14 added together, make iustly without more or lesse 28. Wherefore 28 is a perfect number, and so of others the like. This kinde of numbers is very rare and seldome found. From 1 to 10, there is but one perfect number, namely, 6. From 10 to an 100, there is also but one, that is, 28. Also from 100 to 1000 there is but one which is 496. From 1000 to 10000 likewise but one. So that betwene every stay in numbring, which is euier in the tenth place, there is found but one perfect number And for their rarenes and great perfection, they are of maruelous vse in magike, and in the secret part of philosophy.

Perfect numbers are those which are equal to the sum of their partes. This kinde of numbers is very rare and seldome found.

Number theory after Euclid

Very little for many centuries...

Recall that Diophantus' *Arithmetica* (13 books, c. AD 250) featured number problems; for example [from Lecture IX]:

Problem I.27: *Find two numbers such that their sum and product are given numbers*

The *Arithmetica* also features problems and ideas that we would now classify as number-theoretic; for example:

Problem III.19: *To find four numbers such that the square of their sum plus or minus any one singly gives a square*

Problem V.9: *To divide unity into two parts such that, if a given number is added to either part, the result will be a square*

Restrictions on the permitted form of solutions to problems eventually gave rise to the notion of **Diophantine equations**

Number theory outside Europe

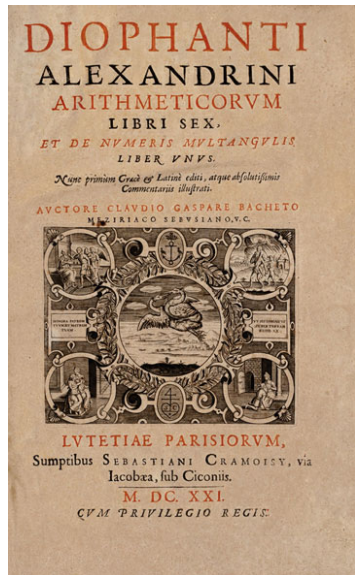
Sūnzǐ Suànjīng 孙子算经 (*The Mathematical Classic of Master Sun*) (3rd–5th century BC) contains a statement, but no proof, of the **Chinese Remainder Theorem** for the solution of simultaneous congruences

An algorithm for the solution was provided by Aryabhata in 6th-century India

In 7th-century India, Brahmagupta studied Diophantine equations (including **Pell's equation** — see later)

These works were unknown in Europe until the 19th century

17th-century number theory



Bachet's Latin edition of
Diophantus' *Arithmetica* (1621)

Pierre de Fermat owned a 1637
edition, which he studied and
annotated

Fermat on number theory

Fermat's Little Theorem: if a is any integer and p is prime then p divides $a^p - a$

Studies of 'Pell's Equation' $x^2 - Dy^2 = 1$

Conjectures on perfect numbers [more in a moment]

Studies of diophantine problems leading to 'Fermat's Last Theorem' [more in a moment]

Published nothing — had to be exhorted to write his ideas down

(See *Mathematics emerging*, §§6.1–6.3)

The 'Last Theorem'

Arithmetica Problem II.8 concerns the splitting of a given square number into two other squares

Fermat's marginal note:

It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain.

(See: Simon Singh, *Fermat's Last Theorem*, Fourth Estate, 1998)

Perfect numbers

Euclid's Theorem: if $2^n - 1$ is prime then $2^{n-1}(2^n - 1)$ is perfect

Fermat to Mersenne (1640): if $2^n - 1$ is prime then n must be prime

Mersenne (1644): if $p \leq 257$ and $2^p - 1$ is prime then p is one of 2, 3, 5, 7, 13, 17, 67 (a misprint for 61 perhaps?), 127, 257. Not quite right: $2^{89} - 1$, $2^{107} - 1$ are prime and $2^{257} - 1$ is composite.

Euler: proof that all even perfect numbers are of Euclid's form (proved 1749, but published posthumously)

(See *Mathematics emerging*, §6.1.2)

NB. 51 Mersenne primes are currently known, the largest being $2^{82,589,933} - 1$ (found in June 2019)

17th-century attitudes to number theory

Fermat failed to spark an interest in number theory in his contemporaries

Pascal to Fermat (1655):

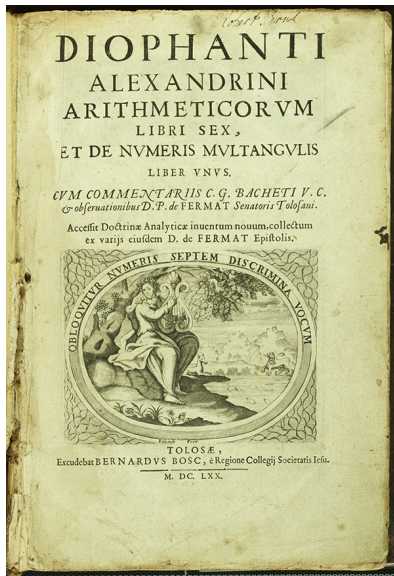
... seek elsewhere those who can follow you in your numerical discoveries ... I confess to you that this goes far beyond me ...

Number-theoretic investigations were widely regarded as trivial and uninteresting

Huygens to Wallis:

There is no lack of better topics for us to spend our time on ...

The 'rebirth' of number theory



1670 edition of Bachet, published by Samuel Fermat, including his father's notes

The 'Last Theorem' was not the only result for which Fermat failed to provide a proof

Number theory was 'reborn' from the attempts of Euler (and later Lagrange and Legendre) to fill the gaps left by Fermat

Euler on number theory

Euler (1747):

Nor is the author disturbed by the authority of the greatest mathematicians when they sometimes pronounce that number theory is altogether useless and does not deserve investigation. In the first place, knowledge is always good in itself, even when it seems to be far removed from common use. Secondly, all the aspects of the truth which are accessible to our mind are so closely related to one another that we dare not reject any of them as being altogether useless. . . .

Consequently, the present author considers that he has by no means wasted his time and effort in attempting to prove various theorems concerning integers and their divisors. . . . Moreover, there is little doubt that the method used here by the author will turn out to be of no small value in other investigations of greater import.

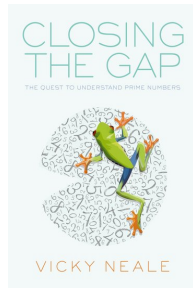
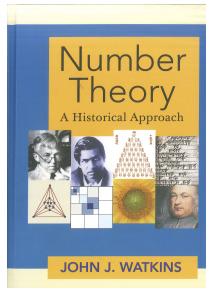
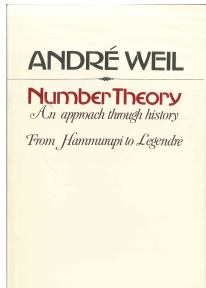
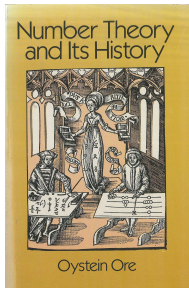
19th-century number theory

Gauss's *Disquisitiones arithmeticae* (1801) became a key text for many years to come: modular arithmetic, quadratic forms, cyclotomy, ...

Number-theoretic problems (especially attempts to prove Fermat's Last Theorem) led to the development of **ideal theory**, and the linking of number theory and abstract algebra in **algebraic number theory**

By the end of the 19th century, a new branch, **analytic number theory**, had also emerged (e.g., Riemann hypothesis, Prime Number Theory $\pi(x) \sim \frac{x}{\log x}, \dots$)

The history of number theory



Leonard Eugene Dickson, *History of the theory of numbers*, 3 vols.,
Carnegie Institution of Washington, 1919–1923: [I](#), [II](#), [III](#)