

O1 History of Mathematics  
Lecture XV  
Geometry and number theory

Monday 26th November 2018  
(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.

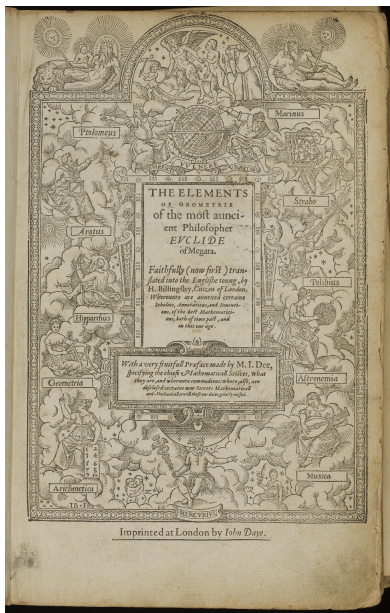
1. A **point** is that which has no part.
2. A **line** is breadthless length.
3. The extremities of a line are points.
4. A **straight line** is a line which lies evenly with the points on itself.
5. A **surface** is that which has length and breadth only.
6. The extremities of a surface are lines.
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  
wishes grace from heaven, and most prosper-  
ous success in all their best attempts and  
exercyses.



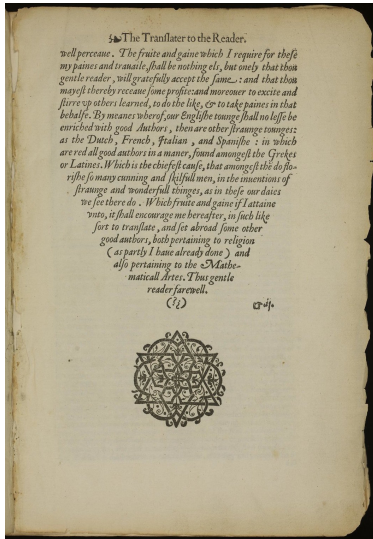
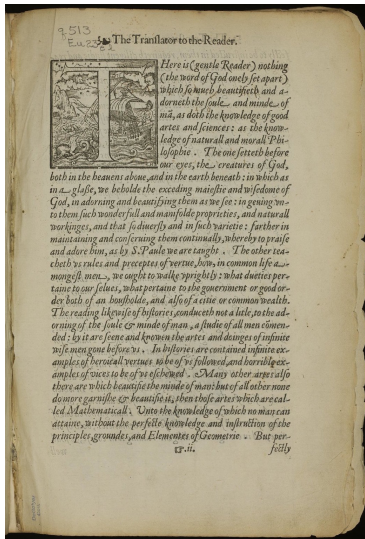
Inaine *Plato*, the great Master  
of many worthy Philosophers,  
and the constant souch, and  
pithy perswader of *Plato*, *Eu-  
clid*, and *Aristo*; in his Schole and  
Academie, sundry times (besides  
his ordinary Scholers) was visited  
of a certaine kinde of men, allured  
by the noble fame of *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 conclude, this *Plato*, *Eu-  
clid*, and *Aristo*, to be Spirituall, Infi-  
nite, 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, for 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, yod in lictif, to  
forewarne his owne Scholers and hearers, both of what matter, and also to what  
code, he stooke 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: By cause, 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 (imitating *Aristo*) will can I  
hope, that according to the ample and dignitie of the *Arts*, & *Mathematices*: I  
am able, either playfully 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

## of Euclides Elementes.

Fol. 314.

will narrow or be narrower, 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, to wit,  $A B C$ , of an every side of the triangle  $A B C$  extend up a straight line, to wit, the side  $A B$ , or rather up the straight line  $A B$  extend upon the side  $A C$  the straight line  $A C$ , and upon the side  $B C$  the straight line  $B C$ , and to beewing the straight lines raised up, their upper ends, the points  $F$  narrow and meet together in one point, to wit, the point  $F$ , and plainly see how these three solid angles, to wit,  $A B C$ ,  $F A C$ , and  $F B C$ , meet together, touching the one the other in the point  $F$ , and to make a solid angle.



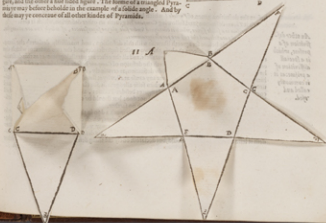
11 A Pyramid is a solide figure contained under many plaine superficieses set upon one plaine superficies, and gathered together to one point.

Teach definition.

Two superficieses raised upon any ground can not make a Pyramid, for that two superficieses laid together in the top, cannot, as before is shewd, make a solid angle. Wherby what the square, the circle, or any other figure, be, as long as they are raised upon one superficies, they cannot make a solid angle. The solid angle is bounded, and terminated by three superficieses, and each superficies is in a top of four sides, and is a top of a square which containeth many sides, either of which is a Pyramid.

And because that all the superficieses of every Pyramid is sliced from one plaine superficies, from the base and ends to one point, or more, or more, to wit, to wit, 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 solid angle, but with three superficieses, but with one round superficies, and each superficies is in a top of four sides, and is a top of a square which containeth many sides, either of which is a Pyramid.

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 superficies, 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 quadrangular Pyramid may be beheld in the example of a solid angle. And by this may it conceive of all other kinds of Pyramids.



# Book I: definitions

## The first booke of Euclides Elementes.



**T**HIS FIRST BOOK is treated of the most simple, easie, and first matters and groundes of Geometry, as to witte, of Lines, Angles, Triangles, Parallels, Squares, and Parallelogrammes. First of the definitions, the way which they use. After that it teacheth how to draw Parallel lines, and how to forme diversitie figures of three sides, & four sides, according to the variety of their sides, and Angles: & comparer them all with Triangles, & also together the one with the other. In all this is taught how a figure of any forme may be changed into a Figure of an other forme. And for that it seemeth of thie most common and generall things, this booke is more universall then is the seconde, third, or any other, and therefore iustly occupieth the first place in order: as that without which, the other bookes of *Euclides* which follow, and also the workes of others which have written in Geometry, cannot be perceived nor understood. And forthwith as all the demonstratours and proofes of all the propositions in this whole booke, depende of these groundes and principles following, which by reason of their playnes neede no great declaration, yet to remove all (be it nearer fo life) obscurity, there are here set certayne thore and manifest expositions of them.

### Definitions.

1. A figure or point is that, which hath no part.

The better to understand what manner of thing a figure or point is, ye must note that the nature and properties of quantitie (when of Geometry extendeth) is to be divided, fo that whatsoever may be divided into sundry partes, is called quantitie. And a point, although it pertaine to quantitie, and hath his being in quantitie, yet it is no quantitie, for that it cannot be divided. Because (as the definition saith), it hath no partes into which it should be divided. So that a point is the least thing that by minde and understanding can be imagined and conceived: then which, there can be nothing else, as the point *A* in the margin.

A figure or point is of *Pythagoras* Scholers after this manner defined. A point is an oval in which hath position. Numbers are conceived in mynde without any forme & figure, and therefore without matter where to receive figure, & consequently without place and position. Wherefore vntie being a parte of number, hath no position, or determinate place. Where by it is manifest, that number is more simple and pure then is magnitude, and also immateriall: and so vntie which is the beginning of number, is lesse materiall then a figure or point, which is the beginning of magnitude. For a point is materiall, and requirerth position and place, and therby differeth from vntie.

2. A line is length without breadth.

There pertaine to quantitie three dimensions, length, breadth, & thickness, or depth, and by these three are all qualities measured & made knowne. There are also, according

The argument of the first booke.

As other definitions of a line.

The endes of a line.

Difference of a point from a line.

Definition of a point.

A.

Definition of a point.

Definition of a line.

## The first Booke

to these three dimensions, three kynde of continuall quantitie; a lyne, a superficies, or plane, and a body. The first kynde, namely a lyne is here defined in these wordes, *a lyne is length without breadth.* A point, for that it is no quantitie nor hath any partes into which it may be divided, but remaineth indivisible, hath not, nor can have any of these three dimension. It neither hath length, breadth, nor thickness. But to a lyne, which is the first kynde of quantitie, is attributed the first dimension, namely, length, and only that, for it hath neither breadth nor thickness, but is conceived to be drawne in length only, and by it, it may be divided into partes as many as ye will, equal or vnequal. But as touching breadth it remaineth indivisible. As the lyne *AB*, which is only drawen in length, may be divided in the point *C* equally, or in the point *D* vnequally, and fo into as many partes as ye will. There are also other, or other, or other, definitions of a lyne: as *A* *B* *C* *D* *B*

As other definitions of a line.

The endes of a line.

Difference of a point from a line.

Definition of a point.

A.

Definition of a point.

Definition of a line.

3 The endes or limites of a lyne, are points.

For a line hath his beginning from a point, and likewise endeth in a point: fo that by this also it is manifest, that points, for their simplicity and lacke of composition, are neither quantitie, nor partes of quantitie, but only the termes and endes of quantitie. As the pointes *a, b, c*, are only the endes of the line *AB*, and no partes thereof. And herein directeth a point in quantitie, from vntie in number: for that although vntie be the beginning of numbers, and no number: as a point is the beginning of quantitie, and no quantitie, yet is vntie a parte of number, for number is nothing else, but a collection of numbers, and therefore may be divided into them, as into his partes. But a point is no part of quantitie, or of a lyne, neither is a lyne composed of points, as number is of vnties. For things indivisible, being neuer fo many added together, can neuer make a thing divisible, as an instant in time, is neither time, nor part of time, but only the beginning and end of time, and couplet & ioyneth partes of vntie together.

4 A right lyne is that which lieth equally betwene his pointes.

As the whole line *AB* lieth straight and equally betwene the pointes *A* *B* without any going up or coming downe on either side.

Compounds and certain others, define a right line thus: *A right line* (wher the shortest extension or draught) is that is or may be drawn from any point to any other, so that the distance betwene them is the least.

A right line is the shortest of all lines, which have one endeth fo the same limites or endes: which is in manner one with the definition of Compounds. As of all their lines *ABC, AD, AC, AEC*, which are all drawen from the point *A*, to the point *C*, as Compounds speaketh, or which have the same limites or endes, as Archimedes saith, the least line limites or endes, as Archimedes saith, the line *ABC*, being a right line, is the shortest.

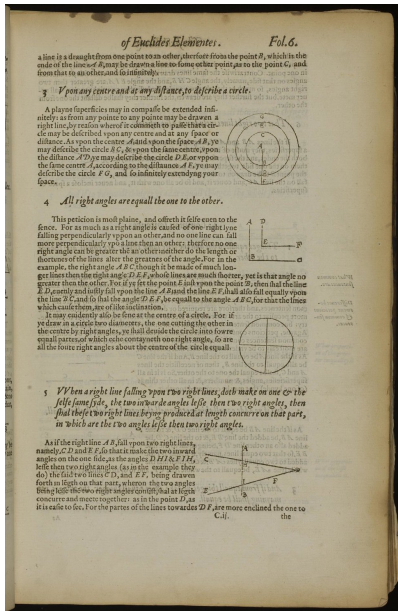
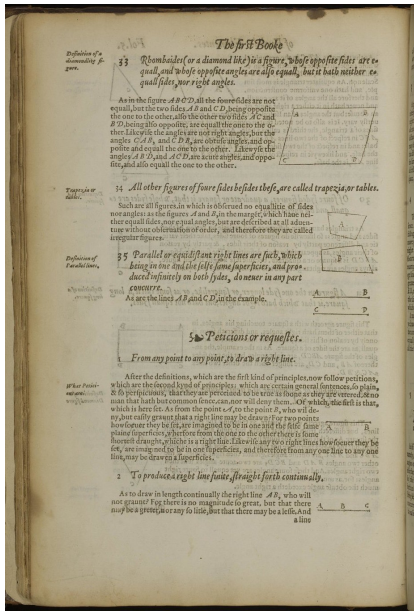
Plato defineth a right line after this manner. *A right line is that whose middle part is like unto its extremes.* As if you put any thing in the middle of a right lyne, you shall not see from the one end to the other, which thing hath ppeneth not in a crooked lyne. The Eclipse of the Sunne (say Astronomers) then happeneth, when the Sunne, the Moone, & our eye are in one right line. For the Moone then being in the middle betwene vs and the Sunne, casteth it to be darkened. Divers other define a right line diversely, as followeth.

A point is that which hath no parts, nor is it a body, nor is it a figure, nor is it a superficies. A point is that which hath no parts, nor is it a body, nor is it a figure, nor is it a superficies.





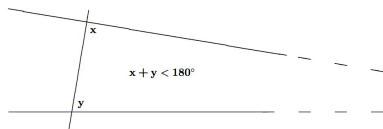
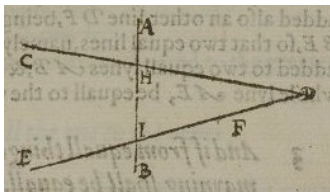
# Book I: postulates





## 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

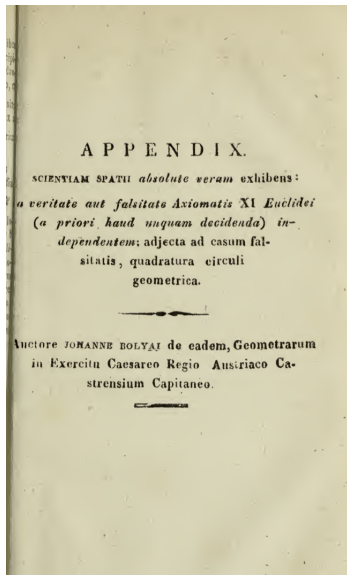
Consistent non-Euclidean geometry probably first constructed (tentatively) by Gauss, c. 1817–1830, but remained unpublished

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)

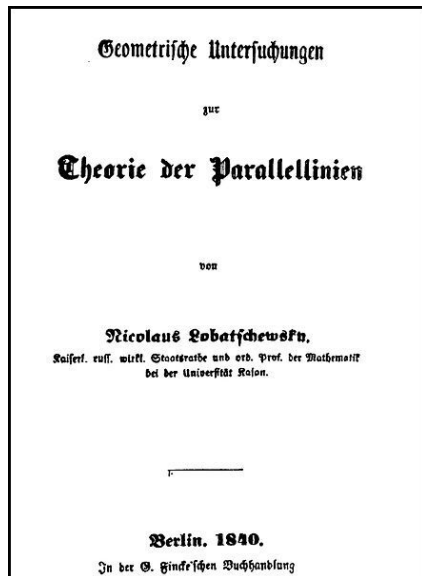
## Meanwhile in Russia...



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

# Euclid on numbers (positive integers)

The first definition

Without doubt should be considered of numbers

Another definition of unity

The second definition

The third definition

The fourth definition

The fifth definition

The sixth definition

The seventh definition

## The seventh Book Definitions

1 **Unit** is that, whereby every thing that is, is said to be one.

As a point is magnitude, so the least thing is magnitude, and no magnitude at all, for the greater and the lesser are in it, as in a unit, a magnitude or number, the least thing is number, and no number at all, and yet the greater and beginning of all numbers. And therefore it is here in this place, of *Euclid* first defined as in the first book, by the like reason and cause was a point, whereby every thing there, is divided and separated from its other, and remaneth on in itself pure and distinct, without addition, subtraction, and in its condition. And where confusion is shown in one order, and any thing on the other, I have known either what it is, or what the nature, and what are the properties thereof, while there are several names of it, that is every thing therefore in that is, *Euclid* hath very spely, *Euclid* hath very spely, that it is, for that it is on a number, according wherewith *Euclid* in that most excellent and absolute work of *Archimedes* which he wrote, doth much value other matters.

*Euclid* hath very spely, that it is, for that it is on a number, according wherewith *Euclid* in that most excellent and absolute work of *Archimedes* which he wrote, doth much value other matters.

2 **Number** is a multitude composed of units.

As the number of three, is a multitude composed and made of three units. Likewise the number eight, is likewise made of eight units, and so forth. For the number of three, is a multitude composed and made of three units. Likewise the number eight, is likewise made of eight units, and so forth. For the number of three, is a multitude composed and made of three units. Likewise the number eight, is likewise made of eight units, and so forth.

3 **Prime number** is that which is not contained by any other number, but itself.

4 **Composite number** is that which is contained by some other number, besides itself.

5 **Even number** is that which is contained by two equal parts.

6 **Odd number** is that which is not contained by two equal parts.

## of Euclides Elementes. Fol. 184.

1 **A part** is a lesse number in comparison to the greater, when the lesse measureth the greater.

2 **Partes are a lesse number in respect of the greater, when the lesse measureth not the greater.**

3 **Multiplex is a greater number in comparison of the lesse, when the lesse number measureth the greater number.**

4 **An even number is that, which may be divided into two equal partes.**

5 **An odd number is that, which may not be divided into two equal partes.**

6 **Prime number** is that which is not contained by any other number, but itself.

7 **Composite number** is that which is contained by some other number, besides itself.

8 **Even number** is that which is contained by two equal partes.

9 **Odd number** is that which is not contained by two equal partes.

10 **Prime number** is that which is not contained by any other number, but itself.

The third definition

The fourth definition

The fifth definition

The sixth definition

The seventh definition

The eighth definition

# The Euclidean algorithm (Proposition VII.2)

## The seventh Book

189.17  
 multiple number B A, wherefore it also measurith this which remaineth nexte, 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 second. And the residue of the second, wherefore also it measurith D G by the 5. common fence of the second. And it is thus, if the residue be G F, therefore it also measurith the whole A F, by the first common fence of the second. And it measurith G C, wherefore it measurith the whole C D, by the first common fence of the second. And it measurith H B by the 5. common fence of the second. And it shall proceed thus continually, wherefore also it measurith the whole number A B by the first common fence of the second. 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 life 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, it 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 the number C D either measurith the number A B or not. If C D measurith A B, it shall be A . . . . . B such it self. Wherefore C D is a common measure of the numbers A . . . . . B C D and A B, which is manifestly also 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 by the 5. common fence. For if there be left out, the said 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 by the continual subtraction of the life from the one 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

This case is the hypothesis. The first case. The second case. The third case.

## of Euclides Elementes Fol. 189.

as often as you can leave a life there it self is namely, C E. And suppose that C D do not measure A E, that there remaineth nothing. Then I say that C E is a common measure to the numbers 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 D 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. That C F is the greatest common measure to the numbers A B and C D.

If also that it 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 both the 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.

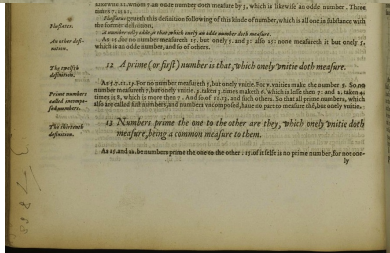
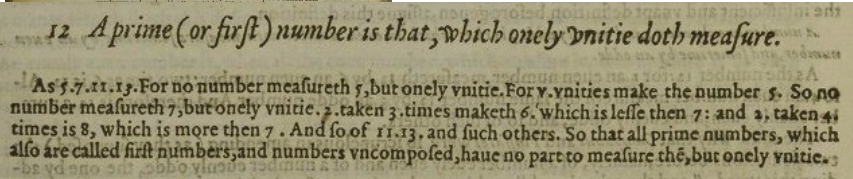
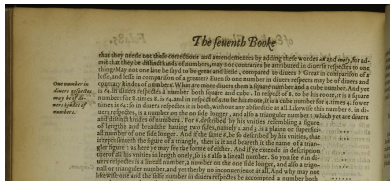
Propose the three numbers given not prime the one to the other, it be A B, C. Now it is required to finde out the said numbers A . . . . . B C D. Let A B, C. To finde out the greatest common measure, let the greatest common measure of the two numbers A and B be D (by the 2. of the seventh) which let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

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 and B, 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

This case is the hypothesis. The first case.

the number C, and 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

# Euclid on prime numbers



# 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  $A$  measureth  $D$ , but it also measureth it not, which is impossible. Wherefore it is impossible to finde out a fourth number proportionall, with these numbers  $A, B, C$ , whensoever  $A$  measureth 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 not 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 measureth 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 measureth  $D E$ : and it also measureth 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 seuen numbers how many soeuer be added together: the whole shall be euē.

E.E.ij.      Suppōit

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 measureth 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 measureth  $D E$ : and it also measureth 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	$D \cdot F$
$G$ .....	

# Euclid on perfect numbers

is double to 3; and to 4 double to 3. Likewise these four numbers are in like proportion 9:4:18:12. For what part is 9 of 3, such part is 18 of 6; as a third part, so is 18 of 6; as a third part. So are these four numbers also in proportion 4:2:12:6: for what part are 4 of 2, such part are 12 of 6; as two third parts, so are 12 of 6; as two third parts. Likewise of 12 are two third parts. Moreover, these numbers are in proportion for what part are these many parts of 6, such 6; for many parts are 12 of 6; as two third parts; for one third part of 6 is 2, which take four times make 8; so 12 is 2 of 3, 18 is four third parts; for one third part of 18, which when foure times make 12. And to converse use of make

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 euer 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 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 euer 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.

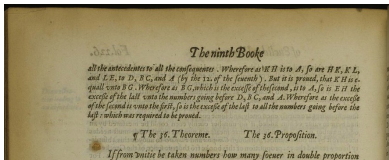
This kinde of numbers called perfect numbers

A number consisting of whole partes being all added together make more then the whole number whose partes they are, as 12 is an abundant number: For all the partes of 12, namely, 1, 2, 3, 4, 6, and

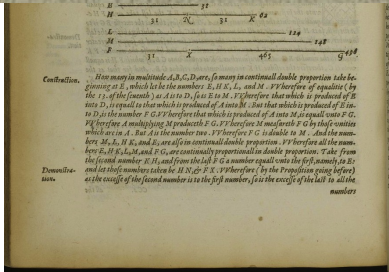
Perfect numbers are those numbers which are equal to the sum of their partes. As 6 is a perfect number, because 1 + 2 + 3 = 6. Likewise 28 is a perfect number, because 1 + 2 + 4 + 7 + 14 = 28. This kinde of numbers is very rare and seldome found.



# Euclid on perfect numbers (Proposition IX.36)



If from vnitie be taken numbers how many soeuer in double proportion continually, vntill the whole added together be a prime number, and if the whole multiplying the last produce any number, that which is produced is a perfecte number.



In modern terms: if  $2^n - 1$  is prime, then  $2^{n-1}(2^n - 1)$  is perfect



## 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

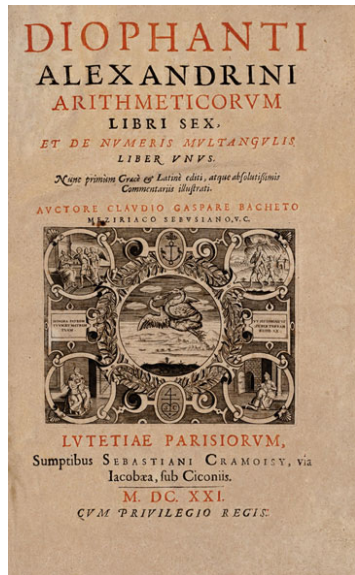
*Sūnzǐ Suànjīng* 孙子算经 (*The Mathematical Classic of Master Sun*) (3rd–5th century BC) contains a statement, but no proof, of the **Chinese Remainder Theorem** for the solution of simultaneous congruences

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. 50 Mersenne primes are currently known, the largest being  $2^{77,232,917} - 1$  (found in January 2018)

## 17th-century attitudes to number theory

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

Pascal to Fermat (1655):

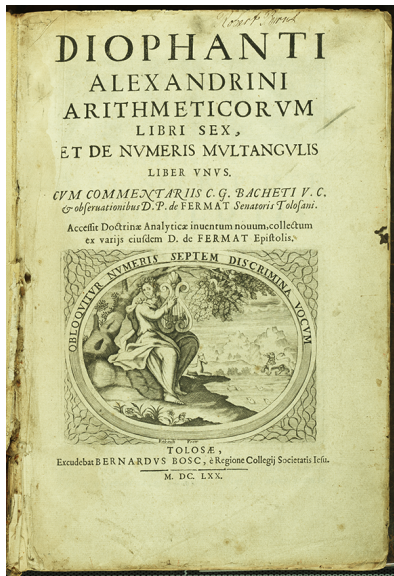
*... seek elsewhere those who can follow you in your numerical discoveries ... I confess to you that this goes far beyond me ...*

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.*

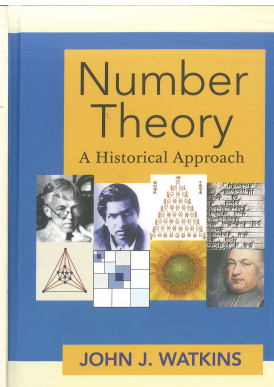
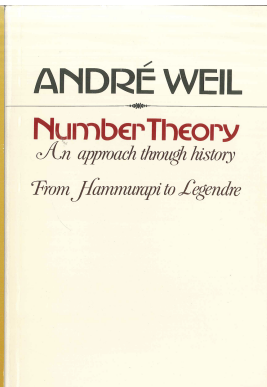
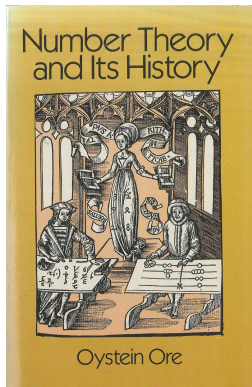
## 19th-century number theory

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](#)