

BO1 History of Mathematics
Lecture XIV
Geometry and number theory

MT 2021 Week 7

Summary

Part 1

- ▶ Euclid's *Elements* revisited
- ▶ The parallel postulate
- ▶ Non-Euclidean geometry

Part 2

- ▶ Number theory down the centuries

Euclid's *Elements*

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

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.

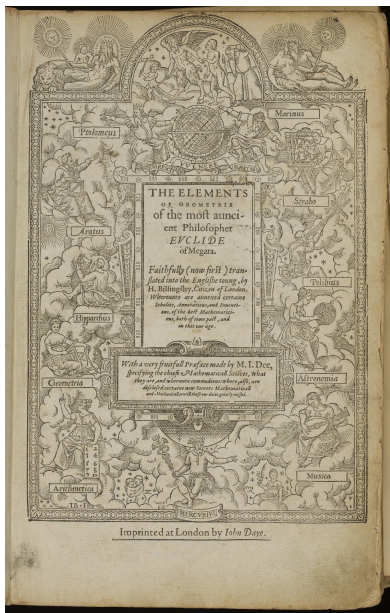
1. A **point** is that which has no part.
2. A **line** is breadthless length.
3. The extremities of a line are points.
4. A **straight line** is a line which lies evenly with the points on itself.
5. A **surface** is that which has length and breadth only.
6. The extremities of a surface are lines.
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 **rectilineal**.
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](#)

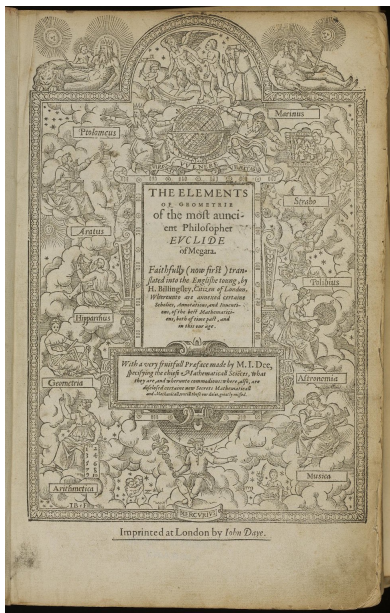
Billingsley's Euclid, 1570



The Elements of Geometrie:

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

Billingsley's Euclid, 1570

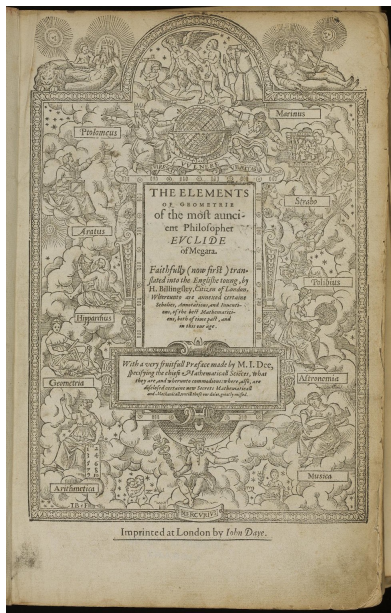


The Elements of Geometrie:

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

Available online

Billingsley's Euclid, 1570



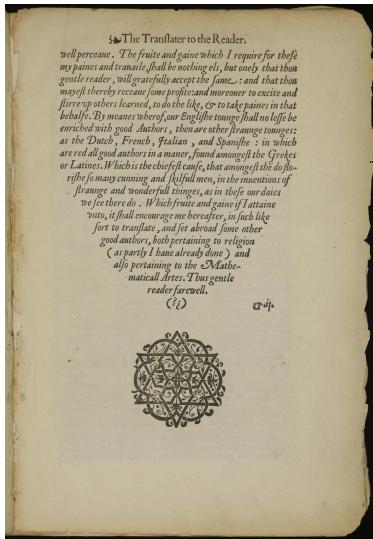
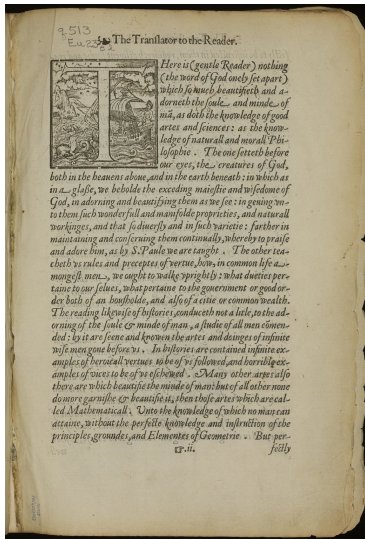
The Elements of Geometrie:

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

[Available online](#)

Preface by John Dee

Billingsley's Preface, pp. 1, 3



Book I: definitions

The first booke of Euclides Elementes.



THE FIRST BOOK is treated of the most simple, easie, and first matters and groundes of Geometry, as to wit, of Lines, Angles, Triangles, Parallels, Squares, and Parallelogrammes. First of these definitions, they say what they are. After that it teacheth how to draw Parallel lines, and how to describe divers figures of three sides, & four sides, according to the variety of their sides, and Angles: & compareth 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 that is somewhat of the most common and generall things, this booke is more vniuersall 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 *Euclid* which follow, and also the workes of others which have written in Geometry, cannot be perceived nor vnderstanded. 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 (ye it neuer be like) 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 vnderstand what manner of thing a figure or point is, ye must note that the nature and properties of quantitie when of Geometry entaileth iust to be decided, first that whatsoever may be deuided 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 deuided. Because (as the definition saith), it hath no partes into which it should be deuided. So that a point is the least thing that by minde and vnderstanding can be imagined and consueued: then which, there can be nothing like, as the point *A* in the margin.

A figure or point is of *Pythagoras* Scholers after this manner defined. A *point* is an *ovine* in which hath position. Numbers are conceived in mynde without any forme & figure, and therefore without matter when to recreate figure, & consequently without place and position. Wherefore vntie being a part 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 requieth position and place, and thereby 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 quantites measured & made knowne. There are also, according

The ground of the first booke.

An other definition of a line.

The endes of a line.

Difference of a point & line.

Definition of a point.

Definition of a right line.

Definition of a right line.

Definition of a line.

An other definition of a line.

The first Booke

to these three dimensions, three kyndes of continuall quantities: a line, a superficies, or plane, and a body. The first kynde, namely a line is here defined in these wordes, *a line is length without breadth.* A point, for that it is no quantitie nor hath any partes into which it may be deuided but remaineth indiuisible, hath not, nor can haue any of these three dimension. It neither hath length, breadth, nor thickness. But to a line, 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 deuided into partes as many as ye will, equally or vnequall. But as touching breadth it remaineth indiuisible. As the line *AB*, which is only drawen in length, may be deuided in the point *C* equally, or in the point *D* vnequally, and so into as many partes as ye will. There are also other, or other, or other, definitions of a line: as *A* *C* *D* *B* these which follow.

A line is the moving of a *point*, as the motion or draught of a pinne or a penne to your fence maketh a line.
 Any way, *A line* is a magnitude having one onely face or dimension, namely, length, wanting breadth and thickness.

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

For a line hath his beginning from a point, and likewise endeth in a point: so 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 onely 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 part of number, nor number is not vntie, but a collection of numbers, and therefore may be deuided into them, as into his partes. But a point is no part of quantitie, or of a line: neither is a line composed of points, as number is of vnties. For things indiuisible, being neuer so many added together, can neuer make a thing diuisible: as an instant in time, is neither time, nor part of time, but only the beginning and end of time, and couplet & ioynerth partes of time together.

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

As the whole line *AB* lieth straight and equally between 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* is that straight extension or draught that is or may be drawn from one point to another, without any bending or turning.

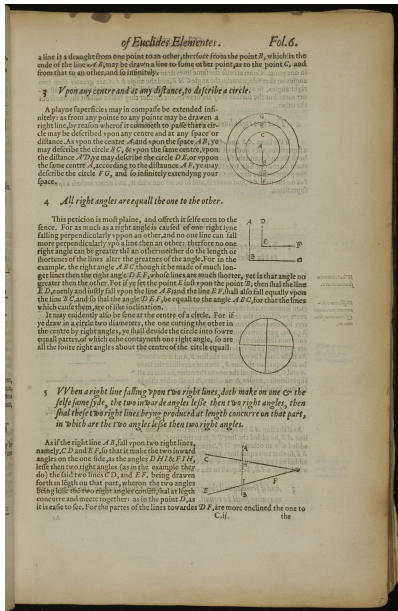
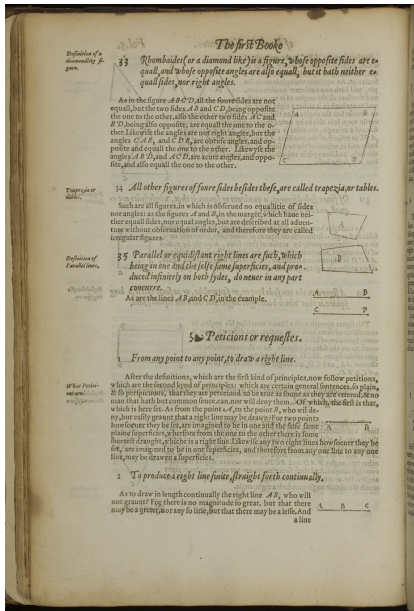
A right line is that straight extension or draught that is or may be drawn from one point to another, without any bending or turning. As if you draw a line from the point *A*, to the point *B*, as *Compounds* speaketh, or which have the self same limites or endes, as *Archimedes* speaketh, the line *AB*, being a right line, is the straight.

Plato defineth a right line after this manner, *A right line* is that whose middle part is equidistant to the endes. As if you put any thing in the middle of a right line, you shall not see from the one end to the other, which thing hath pertaineth not in a crooked line. The Eclipse of the Sunne (say Astronomers) thus 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, causeth it to be darkened. Diuers other define a right line diuersly, as followeth.

A right line is that which hath no other line of itselfe, because it is straight.
 Any way.



Book I: postulates

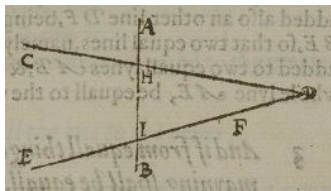


Postulate 5

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.

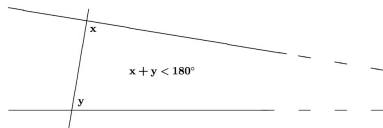
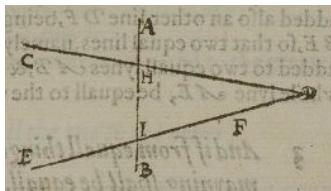
Postulate 5

5 When a right line falling vpon two right lines, doth make on one & the selfe same syde, the two inward 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.



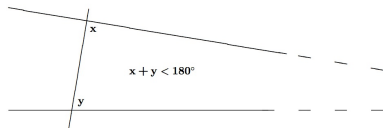
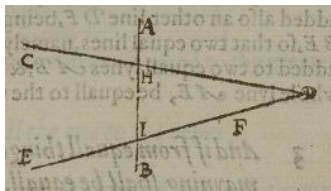
Postulate 5

5 When a right line falling vpon two right lines, doth make on one & the selfe same syde, the two inward 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.



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?

Classical disquiet about the fifth postulate

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

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

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?

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.

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

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:

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

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**

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

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

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

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

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 it the parallel postulate **fails**?

Early hints of non-Euclidean geometry

Giovanni Girolamo Saccheri (1667–1733): sought to establish the validity of Euclidean geometry

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;

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

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

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

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

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

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)



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)



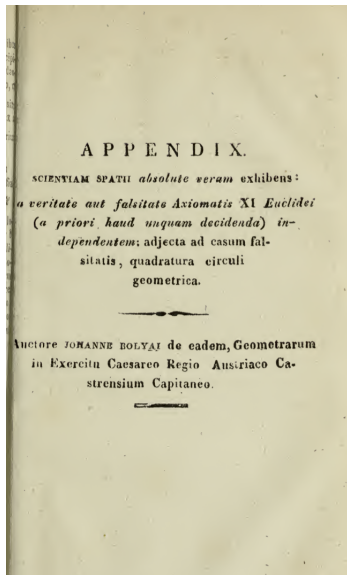
Pursued (against paternal advice) and solved by János Bolyai (1802–1860): “I have created a new and different world out of nothing” (1823)

Bolyai's geometry

He [Farkas Bolyai] gave me the opinion that if I was really successful, I should quickly make a public announcement and that for two reasons. First because the idea might easily pass to someone else who would then publish it; second because, and this is another truth, several things ripen at the same time and appear in different places in the manner of violets coming to light in early spring, and since all scientific striving is like a great war in which one does not know when peace will come, one must win, if possible; for here preeminence comes to him who is first.

Janos Bolyai, 1823 - as quoted in Barrow-Green, Gray & Wilson, Volume 2.

Bolyai's geometry

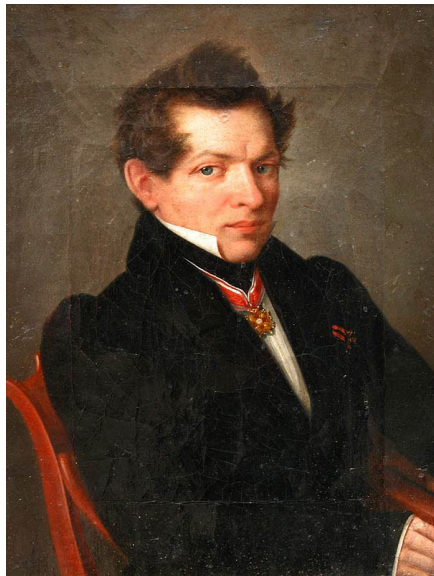


Published as appendix 'The science absolute of space: independent of the truth or falsity of Euclid's axiom XI (which can never be decided a priori)' to father's textbook

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 version of the postulate

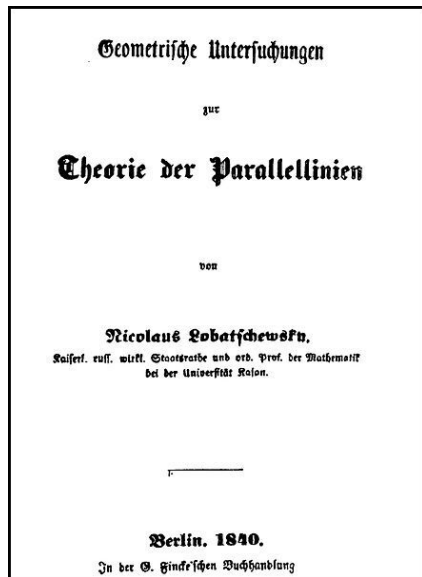
Lobachevskii's works



Complicated story of
dissemination...

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

Lobachevskii's works

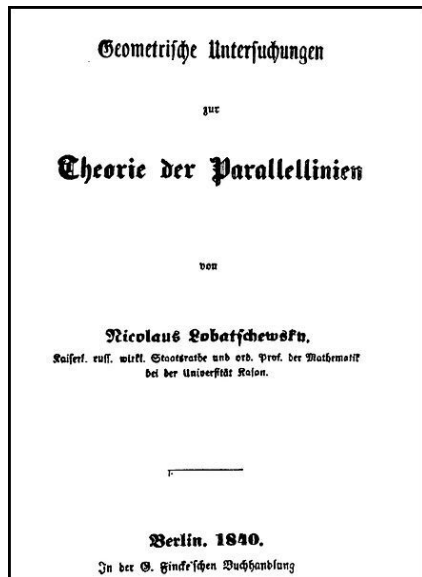


Complicated story of dissemination...

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

Ideas presented in Kazan in 1826, published there 1829

Lobachevskii's works

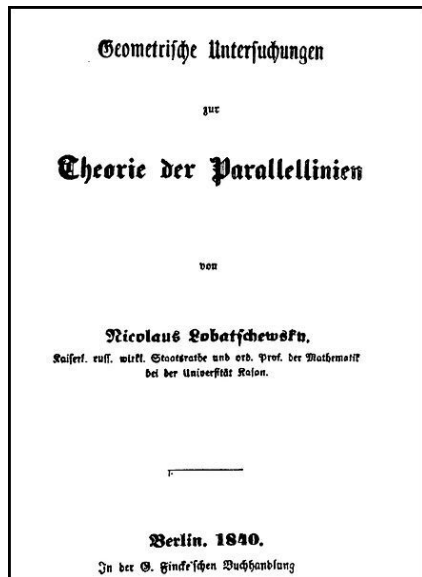


Complicated story of dissemination...

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

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

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

Acceptance and impact of non-Euclidean geometries

Slow to gain acceptance due to

- ▶ obscurity of publications
- ▶ lack of intuitive understanding

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

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

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

Part 2: Early Number Theory

Euclid on numbers

Euclid on numbers (positive integers)

The Euclidean algorithm (Proposition VII.2)

The seventh Book

middle number B A, wherefore it also measurith this which remaineth nexte, the number F A (by the 4. common instance 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 whole number F A, wherefore also E measurith F H, and it measurith also G C, measurith the number F A, wherefore also E measurith F H, and it measurith the whole number F A, wherefore (by the first common instance) it also measurith that which remaineth H A, which is to witte, it self being a number, which is impossible. Wherefore no 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 by the subtraction, all the yeres you come to witte, For if in the continual subtraction there be left before you come to witte, Suppose that H A be the number wherem the life is made, which also being divided out of G C cleaveth nothing. Wherefore H A measurith G C wherefore also it measurith H B by the 1. common instance of the fourth. And the residue of the division is H B, therefore it also measurith the whole A B, by the first common instance of the fourth. And it measurith G C, wherefore it measurith the whole C D, by the first common instance of the fourth. And it measurith H B by the 1. common instance of the fourth. And it shall proceed thus continually, wherefore also it measurith the whole number A B by the first common instance of the fourth. Now for as 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 supposition.

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 the length to witte, then are those numbers given prime the one to the other. But if there be a life before you come to witte, 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 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 $A \dots B \dots C \dots D$ measurith it self. Wherefore C D is a common measure of the numbers $A \dots B \dots C \dots D$ and A B, which is manifestly a 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 $A \dots B \dots B$ and C D, the life be continually taken away from the greater, $C \dots F \dots D \dots D$ there will before you come to witte, the left a number, which will measure the number given before by the 1. common instance. For if there be left out, the said number A B and C D, be prime the one to the other, which is contrary to the supposition. Let the said number left by the continual 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

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 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 instance of the fourth) and it likewise measurith it self, wherefore it also measurith the whole C D (by the sixth common instance of the fourth) but C D measurith B E, wherefore C E also measurith B E (by the fifth common instance of the fourth). And it measurith also A E, wherefore it also measurith the whole B A (by the sixth common instance of the fourth) 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.

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 $A \dots B \dots B$ first of all as G measurith C D, and C D measurith B E, G also measurith B E (by the sixth common instance of the fourth) and it measurith the whole A B, wherefore also it measurith the residue, namely, A E (by the 4. common instance of the fourth). But A E measurith D F, wherefore G also measurith D F (by the first of 5. common instance of the fourth) 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, the numbers A B, C. Now it is required to finde out the said numbers $A \dots B \dots C \dots D$ A B, C to finde out the greatest common measure. Take the greatest common measure of the two numbers A and B (by the 2. of the 7. 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, wherefore D measurith the numbers A B, C. Wherefore D is a common measure unto the numbers A B, C. Now I say that it is the greatest common measure unto them. For if D be not the greatest common measure unto the 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 the

Demons-tration of the second edge.

That C F is a common measure of the numbers A B and C D.

That C F is the greatest common measure of the numbers A B and C D.

Words French.

The reason of this proposition.

How to know whether two numbers be prime the one to the other.

The case in this proposition.

The first edge.

The second edge.

Words French.

How to know whether two numbers be prime the one to the other.

The case in this Proposition.

The first edge.

Euclid on perfect numbers

is double to 3; and to 4 double to 3. Likewise these four numbers are in like proportion 4 to 6, as 6 to 9; for what part 4 is of 3, such part is 6 of 4; and as a third part, so is 9 of 6; of each third part, so are these four numbers also in proportion 4, 6, 9, 12; as 4 is to 6, so 6 is to 9, and 9 is to 12; for as many parts as 4 is of 3, so many parts are 6 of 4, and as many parts as 6 is of 4, so many parts are 9 of 6, and as many parts as 9 is of 6, so many parts are 12 of 9; and as many parts as 12 is of 9, so many parts are 16 of 12; which when four times taken 8 is to 12, as 12 is to 16; four times taken 12 is to 16, as 16 is to 24; which when four times taken 16 is to 24, as 24 is to 32; and so on in like manner.

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, is found in the secret part of philosophy.

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 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, is found in the secret part of philosophy.

A number standing in that 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, 28, 496, &c.

Number theory after Euclid

Very little for many centuries...

Number theory after Euclid

Very little for many centuries...

Recall that Diophantus' *Arithmetica* (13 books, c. AD 250) featured number problems;

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 VIII]:

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

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 VIII]:

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;

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 VIII]:

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*

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 VIII]:

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*

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 VIII]:

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

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

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)

Number theory outside Europe

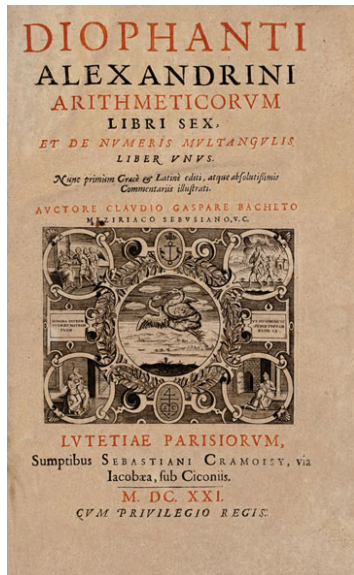
Sūnzǐ Suànjīng 孙子算经 (*The Mathematical Classic of Master Sun*) (3rd–5th century BC) contains a statement, but no proof, of the **Chinese Remainder Theorem** for the solution of simultaneous congruences

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

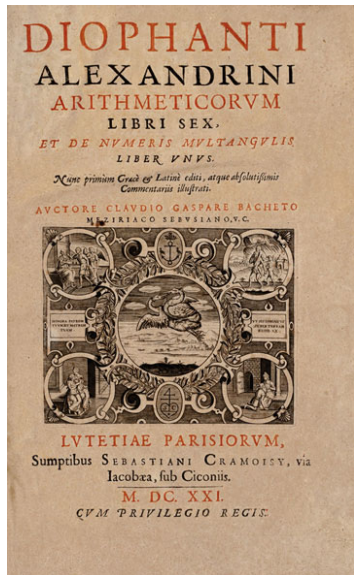
17th-century number theory



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

*Claude Gaspard Bachet de
Méziriac (1581—1638)

17th-century number theory



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

*Claude Gaspard Bachet de
Méziriac (1581—1638)

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 $a^p - a$

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' $x^2 - Dy^2 = 1$

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]

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]

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

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

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

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.

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)

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

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 ...

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

17th-century attitudes to number theory

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

Pascal to Fermat (1655):

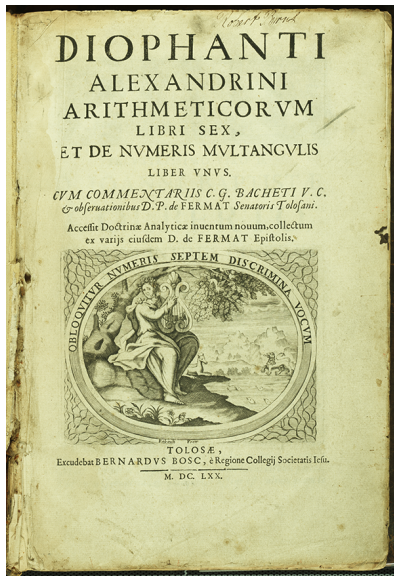
... seek elsewhere those who can follow you in your numerical discoveries ... I confess to you that this goes far beyond me ...

Number-theoretic investigations were widely regarded as trivial and uninteresting

Huygens to Wallis:

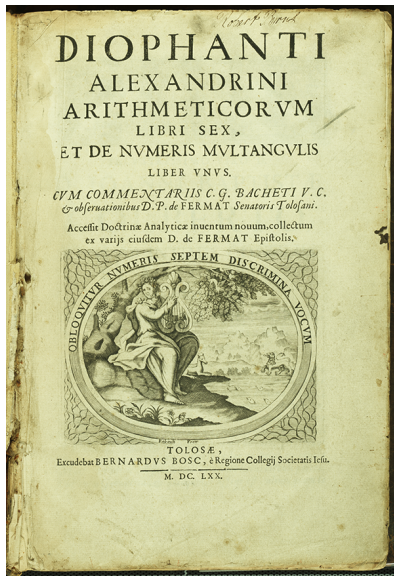
There is no lack of better topics for us to spend our time on ...

The 'rebirth' of number theory



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

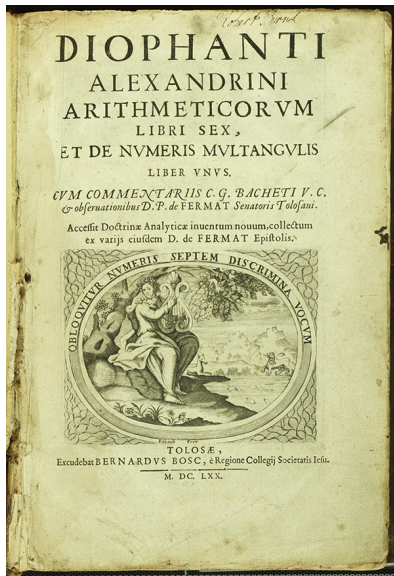
The 'rebirth' of number theory



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

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, ...

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**

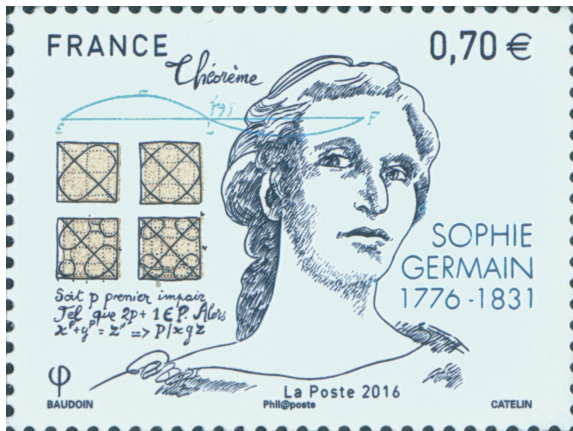
19th-century number theory

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**

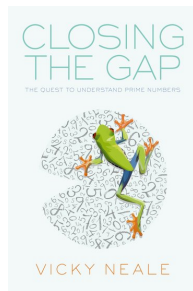
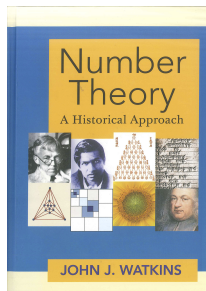
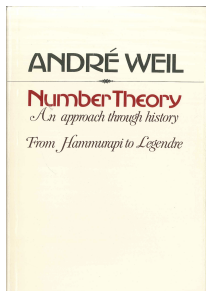
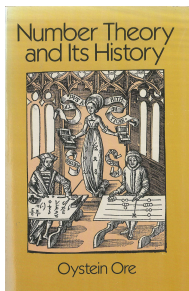
By the end of the 19th century, a new branch, **analytic number theory**, had also emerged (e.g., Riemann hypothesis, Prime Number Theory $\pi(x) \sim \frac{x}{\log x}, \dots$)

Sophie Germain



Arithmetic and Memorial Practices by and Around Sophie Germain in the 19th Century, by Jenny Boucard, In: [Kaufholz-Soldat, E., & Oswald, N. \(2020\). *Against all odds: Women's ways to mathematical research since 1800*, Springer.](#)

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](#)