



Mathematical
Institute

Why study the history of mathematics?

CHRISTOPHER HOLLINGS

*Mathematical Institute & The Queen's College
University of Oxford*

Fridays@2, HT25, Week 6

Oxford
Mathematics



Some possible answers

Studying the history of mathematics

- ▶ humanises and contextualises mathematics
- ▶ makes mathematics more accessible (outreach)
- ▶ can promote diversity in mathematics
- ▶ promotes links between pure and applied mathematics
- ▶ promotes links with other disciplines
- ▶ can highlight different approaches to problem solving
- ▶ helps in understanding why we now do things in a certain way
- ▶ can aid in teaching/learning mathematics
- ▶ can spark new lines of mathematical research
- ▶ is interesting in its own right!

Some possible answers

Studying the history of mathematics

- ▶ humanises and contextualises mathematics
- ▶ makes mathematics more accessible (outreach)
- ▶ can promote diversity in mathematics
- ▶ promotes links between pure and applied mathematics
- ▶ promotes links with other disciplines
- ▶ can highlight different approaches to problem solving
- ▶ helps in understanding why we now do things in a certain way
- ▶ can aid in teaching/learning mathematics
- ▶ can spark new lines of mathematical research
- ▶ is interesting in its own right!

Euclidean mathematics

PROPOSITION 47.

In right-angled triangles the square on the side subtending the right angle is equal to the squares on the sides containing the right angle.

Let ABC be a right-angled triangle having the angle BAC right;

I say that the square on BC is equal to the squares on BA, AC .

For let there be described on BC the square $BDEC$,
and on BA, AC the squares
 GB, HC ; [I. 46]

through A let AL be drawn parallel to either BD or CE , and let AD, FC be joined.

Then, since each of the angles BAC, BAG is right, it follows that with a straight line BA , and at the point A on it, the two straight lines AC, AG not lying on the same side make the adjacent angles equal to two right angles;

therefore CA is in a straight line with AG . [I. 14]

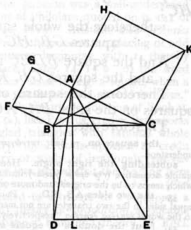
For the same reason

BA is also in a straight line with AH .

And, since the angle DBC is equal to the angle FBA : for each is right:

let the angle ABC be added to each;

therefore the whole angle DBA is equal to the whole angle FBC . [C. N. 2]



Cartesian mathematics

tirer de cete science. Aussi que ie n'y remarque rien de si difficile, que ceux qui feront vn peu versés en la Geometrie commune, & en l'Algebre, & qui prendront garde a tout ce qui est en ce traité, ne puissent trouver.

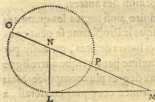
C'est pourquoy ie me contenteray icy de vous avertir, que pourvu qu'en demellant ces Equations on ne manque point a se seruir de toutes les diuisions, qui seront possibles, ou aura infalliblement les plus simples termes, auxquels la question puisse estre reduite.

Quels
sont les
problèmes
plans

Et que si elle peut estre resolue par la Geometrie ordinaire, c'est a dire, en ne se seruant que de lignes droites & circulaires tracées sur vne superficie plate, lorsque la derniere Equation aura esté entierement demeslée, il n'y restera tout au plus qu'un quarré inconnu, esgal a ce qui se produist de l'Addition, ou soustraction de sa racine multipliée par quelque quantité connue, & de quelque autre quantité aussi connue.

Comment
ils
se
resoluent.

Et lors cete racine, ou ligne inconnue se trouue aisément. Car si l'ay par exemple



$x \propto ax + bb$
ie fais le triangle rectangle NLM, dont le costé LM est esgal à b racine quarrée de la quantité connue bb , & l'autre LN est $\frac{1}{2}a$, la moitié de l'autre quantité connue, qui estoit multipliée par x que ie suppose estre la ligne inconnue. puis prolongeant MN la baze de ce triangle,

angle, iusques a O, en sorte qu'NO soit esgale a NL, la toute OM est x la ligne cherchée. Et elle s'exprime en cete forte

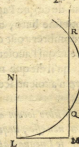
$$x \propto \frac{1}{2}a + \sqrt{\frac{1}{4}aa + bb}.$$

Que si i'ay $y \propto -ay + bb$, & que y soit la quantité qu'il faut trouver, ie fais le mesme triangle rectangle NLM, & de sa baze MN i'oste NP esgale a NL, & le reste PM est y la racine cherchée. De façon que i'ay $y \propto -\frac{1}{2}a + \sqrt{\frac{1}{4}aa + bb}$. Et tout de mesme si l'auios $x \propto -ax + b$, PM seroit x . & i'aurois

$$x \propto \sqrt{-\frac{1}{2}a + \sqrt{\frac{1}{4}aa + bb}} \text{ \& ainsi des autres.}$$

Enfin si l'ay

$$x \propto ax - bb:$$



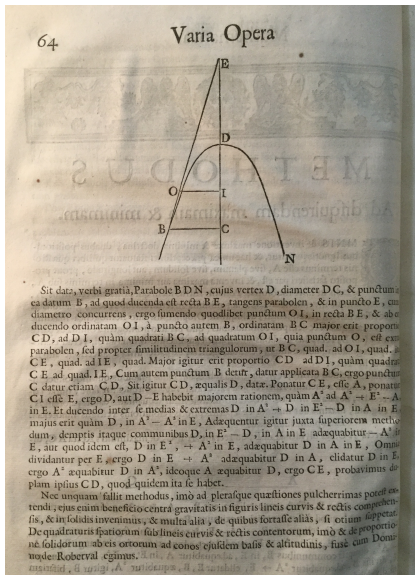
ie fais NL esgale à $\frac{1}{2}a$, & LM esgale à b côme deuant, puis, au lieu de ioindre les points MN, ie tire MQR parallele a LN, & du centre N par L ayant descrit vn cercle qui la coupe aux points Q & R, la ligne cherchée x est MQ, oubié MR, car en ce cas elle s'ex-

prime en deux façons, a sçauoir $x \propto \frac{1}{2}a + \sqrt{\frac{1}{4}aa - bb}$, & $x \propto \frac{1}{2}a - \sqrt{\frac{1}{4}aa - bb}$.

Et si le cercle, qui ayant son centre au point N, passe par le point L, ne coupe ny ne touche la ligne droite MQR, il n'y a aucune racine en l'Equation, de façon qu'on peut assurer que la construction du probleme proposé est impossible.

Au

Fermat's tangent method

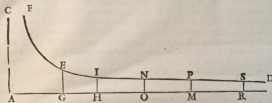


Worked out c. 1629, but only published posthumously in *Varia opera mathematica*, 1679

Fermat's quadrature of higher hyperbolas

lùm quadrata, cubos, quadratoquadrata, &c. quarum exponentes sunt. 2. 3. & 4. &c. sed etiam latera simplicia, quorum exponentes est unitas, Aio itaque omnes in infinitum huiusmodi hyperbolas, unicâ demptâ, quæ Apolloniana est, sive primaria, beneficio proportionis geometricæ uniformis & perpetuæ methodo quadrari possit.

Exponatur, si placet, hyperbola, cuius ea sit proprietas, ut fit semper ut quadratum rectæ HA, A, ad quadratum rectæ AG, ita recta GE, ad rectam HI, & ut quadratum



OA, ad quadratum AH, ita recta HI, ad rectam ON, &c. Aio spatium infinitum, cuius basis GE, & curva ES, ex uno latere, ex alio vero asymptotus infinita OR, æquari spatium rectilineo dato. Fingantur termini progressionis geometricæ in infinitum extendendi, quorum primus sit AG, secundus AH, tertius AO, &c. in infinitum, & ad sic per approximationem tantum accedant quantum satis fit ut iuxta Methodum Archimedeam, parallelogrammum rectilineum sub GE, in GH, quadrilincum mixto GHE, adequetur, ut loquitur Diophantus, aut ferè æquetur.

GE, in GH.

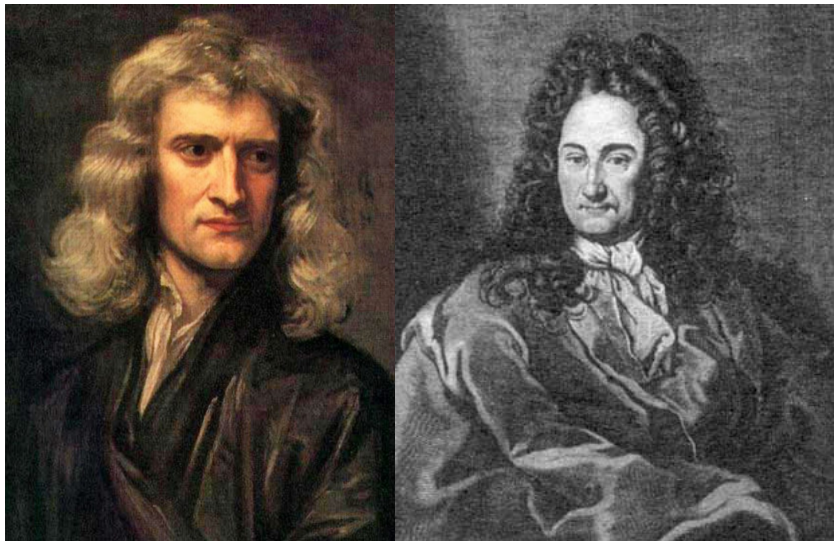
Item ut priora ex intervallis rectis proportionalium GH, HO, OM, & similia sint ferè inter se aequalia, ut commodè per *ἀναγωγή in ἀδύναμιν*, per circumscriptiones & inscriptiones Archimedea demonstrandi ratio institui possit, quod semel monuisse sufficit, ne artificium quibilibet geometris jam satis notum inculcare sæpius & iterare cogamur.

His positis, cum sit ut AG, ad AH, ita AH, AO, & ita AO ad AM, erit pariter ut AG, ad AH: ita intervallum GH, ad HO, & ita intervallum HO, ad OM, &c. Parallelogrammum autem sub EG, in GH, erit ad parallelogrammum sub HI, in HO, ut parallelogrammum sub HI, in HO, ad parallelogrammum sub NO, in OM, cum enim ratio parallelogrammi sub GE, in GH, ad parallelogrammum sub HI, in HO, componatur ex ratione rectæ GE, ad rectam HI, & ex ratione rectæ GH, ad rectam HO: fit autem ut GH, ad HO, ita AG, ad AH, ut proximumimus. Ergo ratio parallelogrammi sub EG, & GH, ad parallelogrammum sub HI, in HO, componitur ex ratione GE, ad HI, & ex ratione AG, ad AH, sed ut GE, ad HI, ita ex constructione HA, quadratum, ad quadratum GA, sive propter proportionales: ita recta AO, ad rectam GA. Ergo ratio parallelogrammi sub EG, in GH, ad parallelogrammum sub HI, in HO, componitur ex ratione AO, ad AG, & AG, ad AH, sed ratio AO ad AH, componitur ex illis duobus. Ergo parallelogrammum sub GE, in GH, est ad parallelogrammum sub HI, in HO, ut OA, ad HA: sive ut HA, ad AG.

Similiter probabitur parallelogrammum sub HI, in HO, esse ad parallelogrammum sub ON, in OM, ut AO, ad HA, sed tres rectæ quæ constituunt rationes parallelogrammorum, rectæ nempe AO, HA, GA, sunt proportionales ex constructione.

Worked out in the early 1640s, but only published posthumously in *Varia opera mathematica*, 1679

The birth of calculus



Newton's method of fluxions

12. Ex. 5. As if the Equation $zx + axz - y^2 = 0$ were propos'd to express the Relation between x and y , as also $\sqrt{ax - xx} = BD$, for determining a Curve, which therefore will be a Circle. The Equation $zx + axz - y^2 = 0$, as before, will give $2zx + axz + axz - 4yy^2 = 0$, for the Relation of the Celerities \dot{x} , \dot{y} , and \dot{z} . And therefore since it is $z = x \times BD$ or $z = x \sqrt{ax - xx}$, substitute this Value instead of it, and there will arise the Equation $2xz + axz \sqrt{ax - xx} + axz - 4yy^2 = 0$, which determines the Relation of the Celerities \dot{x} and \dot{y} .

DEMONSTRATION of the Solution.

13. The Moments of flowing Quantities, (that is, their indefinitely small Parts, by the accession of which, in indefinitely small portions of Time, they are continually increas'd,) are as the Velocities of their Flowing or Increasing.

14. Wherefore if the Moment of any one, as x , be represented by the Product of its Celerity \dot{x} into an indefinitely small Quantity o (that is, by $\dot{x}o$), the Moments of the others y , z , will be represented by $\dot{y}o$, $\dot{z}o$; because $\dot{y}o$, $\dot{x}o$, $\dot{z}o$, are to each other as \dot{y} , \dot{x} , \dot{z} , and o .

15. Now since the Moments, as $\dot{x}o$ and $\dot{y}o$, are the indefinitely little accessions of the flowing Quantities x and y , by which those Quantities are increased through the several indefinitely little intervals of Time; it follows, that those Quantities x and y , after any indefinitely small interval of Time, become $x + \dot{x}o$ and $y + \dot{y}o$. And therefore the Equation, which at all times indifferently expresses the Relation of the flowing Quantities, will as well express the Relation between $x + \dot{x}o$ and $y + \dot{y}o$, as between x and y : So that $x + \dot{x}o$ and $y + \dot{y}o$ may be substituted in the same Equation for those Quantities, instead of x and y .

16. Therefore let any Equation $ax^2 - az^2 + axy - y^2 = 0$ be given, and substitute $x + \dot{x}o$ for x , and $y + \dot{y}o$ for y , and there will arise

$$\left. \begin{aligned} &x^2 + 2\dot{x}x\dot{o} + 3\dot{x}^2\dot{o}\dot{o} + \dot{x}^3\dot{o}^3 \\ &- az^2 - 2a\dot{z}z\dot{o} - a\dot{z}^2\dot{o}^2 \\ &+ axy + a\dot{x}y\dot{o} + a\dot{y}x\dot{o} + a\dot{x}\dot{y}\dot{o}\dot{o} \\ &- y^2 - 2\dot{y}y\dot{o} - 3\dot{y}^2\dot{o}\dot{o} - \dot{y}^3\dot{o}^3 \end{aligned} \right\} = 0.$$

17. Now by Supposition $x^2 - az^2 + axy - y^2 = 0$, which therefore being expunged, and the remaining Terms being divided by o , there will remain $2\dot{x}x + 3\dot{x}^2\dot{o} + \dot{x}^3\dot{o}^2 - 2a\dot{z}z - a\dot{z}^2\dot{o} - \dot{a}\dot{y}x + a\dot{x}y + a\dot{x}\dot{y}\dot{o} - 2\dot{y}y - 3\dot{y}^2\dot{o} - \dot{y}^3\dot{o}^2 = 0$. But whereas o is supposed to be infinitely little, that it may represent the Moments of Quantities; the Terms that are multiply'd by it will be nothing in respect of the rest. Therefore I reject them, and there remains $2\dot{x}x - 2a\dot{z}z + a\dot{x}y + a\dot{y}x - 2\dot{y}y = 0$, as above in Examp. 1.

18. Here we may observe, that the Terms that are not multiply'd by o will always vanish, as also those Terms that are multiply'd by o of more than one Dimension. And that the rest of the Terms being divided by o , will always acquire the form that they ought to have by the foregoing Rule: Which was the thing to be proved.

19. And this being now shewn, the other things included in the Rule will easily follow. As that in the propos'd Equation several flowing Quantities may be involved; and that the Terms may be multiply'd, not only by the Number of the Dimensions of the flowing Quantities, but also by any other Arithmetical Progressions; so that in the Operation there may be the same difference of the Terms according to any of the flowing Quantities, and the Progression be dispos'd according to the same order of the Dimensions of each of them. And these things being allow'd, what is taught besides in Examp. 3, 4, and 5, will be plain enough of itself.

PROB. II.

An Equation being propos'd, including the Fluxions of Quantities, to find the Relations of those Quantities to one another.

A PARTICULAR SOLUTION.

1. As this Problem is the Converse of the foregoing, it must be solved by proceeding in a contrary manner. That is, the Terms multiply'd by \dot{x} being dispos'd according to the Dimensions of x , they must be divided by \dot{x} , and then by the number of their Dimensions, or perhaps by some other Arithmetical Progression. Then the same work must be repeated with the Terms multiply'd by \dot{y} , \dot{z} , or

See the Analysis des infinitesimales petites de the M. de l'Hospital.

Newton's method of fluxions

We begin with a **fluent** quantity x , assumed implicitly to depend upon some independent variable, and we seek the **fluxion** \dot{x} , i.e., the rate of change of x with respect to the independent variable

Newton employed the notion of a **moment** o , an 'indefinitely small Quantity'

When the independent variable changes by o , x changes by $\dot{x}o$

Newton's method of fluxions

We seek the fluxion of the equation $x^3 - ax^2 + axy - y^3 = 0$

Substitute $x + \dot{x}o$ for x and $y + \dot{y}o$ for y , and expand:

$$\left. \begin{array}{r} x^3 + 3\dot{x}ox^2 + 3\dot{x}^2oox + \dot{x}^3o^3 \\ - ax^2 - 2a\dot{x}ox - a\dot{x}^2oo \\ + axy + a\dot{x}oy + a\dot{y}ox + a\dot{x}\dot{y}oo \\ - y^3 - 3\dot{y}oy^2 - 3\dot{y}^2ooy - \dot{y}^3o^3 \end{array} \right\} = 0$$

Newton's method of fluxions

We seek the fluxion of the equation $x^3 - ax^2 + axy - y^3 = 0$

Substitute $x + \dot{x}o$ for x and $y + \dot{y}o$ for y , and expand:

$$\left. \begin{array}{r} + 3\dot{x}ox^2 + 3\dot{x}^2o^2x + \dot{x}^3o^3 \\ - 2a\dot{x}ox - a\dot{x}^2oo \\ + a\dot{x}oy + a\dot{y}ox + a\dot{x}\dot{y}oo \\ - 3\dot{y}oy^2 - 3\dot{y}^2o^2y - \dot{y}^3o^3 \end{array} \right\} = 0$$

Newton's method of fluxions

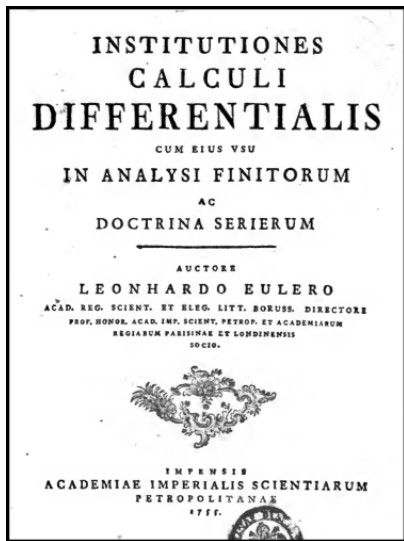
We are left with $3\dot{x}x^2 + 3\dot{x}^2ox + \dot{x}^3oo - 2a\dot{x}x - a\dot{x}^2o + a\dot{x}y + a\dot{y}x + a\dot{x}yo - 3\dot{y}y^2 - 3\dot{y}^2oy - \dot{y}^3oo = 0$

'But whereas o is supposed to be infinitely little, [...] the Terms that are multiply'd by it will be nothing in respect of the rest'

What remains is $3\dot{x}x^2 - 2a\dot{x}x + a\dot{x}y + a\dot{y}x - 3\dot{y}y^2 = 0$

(Recall that we started with $x^3 - ax^2 + axy - y^3 = 0$)

Calculus systematised

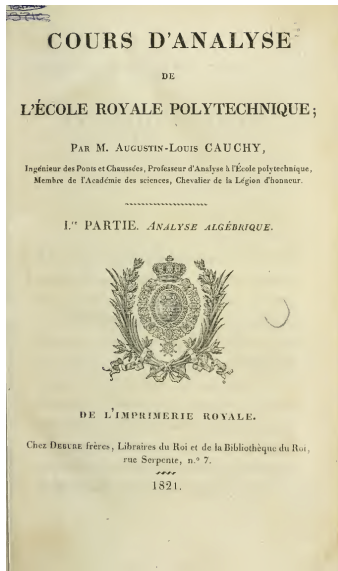


Leonhard Euler, *Introductio in
analysin infinitorum*, Lausanne,
1748

—, *Institutiones calculi
differentialis*, St Petersburg, 1755

—, *Institutiones calculi integralis*,
3 vols, St Petersburg, 1768–1770

Cauchy's *Cours d'analyse* (1821)



Cauchy sequences

Cours d'analyse, pp. 124–125:

In order for the series u_0, u_1, u_2, \dots [that is, $\sum u_j$] to be convergent [...] it is necessary and sufficient that the partial sums

$$s_n = u_0 + u_1 + u_2 + \&c. \dots + u_{n-1}$$

converge to a fixed limit s : in other words, it is necessary and sufficient that for infinitely large values of the number n , the sums

$$s_n, s_{n+1}, s_{n+2}, \&c. \dots$$

differ from the limit s , and consequently from each other, by infinitely small quantities.

Continuity

In *Cours d'analyse*, p. 34, Cauchy defined a function f to be **continuous** between certain limits if, for each x between those limits, the value of $f(x)$ is unique and finite, and $|f(x + \alpha) - f(x)|$, where α is indefinitely small, decreases indefinitely with α .

In other words (p. 35): for x between the given limits, an infinitely small increase in x produces an infinitely small increase in $f(x)$

So Cauchy defined continuity **on an interval**, rather than at a point (and similarly elsewhere, when defining convergence)

He went on to derive basic results concerning continuous functions: that the composition of two continuous functions is continuous, the Intermediate Value Theorem, etc.

A theorem of Cauchy

Cauchy, *Cours d'analyse*, pp. 131–132:

When the various terms of a series are functions of a variable x , continuous with respect to this variable in the neighbourhood of a particular value for which the series is convergent, the sum s of the series is also, in the neighbourhood of this value, a continuous function of x .

In other words: a convergent series of continuous functions converges to a continuous function.

Not true!

Cauchy's argument

Cauchy considered a sequence of continuous functions $u_0(x), u_1(x), u_2(x), \dots$ on a given interval. He supposed that the corresponding series converges to a function $s(x)$. Partial sums are denoted by $s_n(x) = \sum_{j=0}^{n-1} u_j(x)$. The n th remainder term $r_n(x)$ is defined by $s(x) = s_n(x) + r_n(x)$.

Cauchy noted that each s_n is evidently continuous for values of x in the given interval. Suppose that we increase x by an infinitely small quantity α . For all values of n , the corresponding increase in $s_n(x)$ will also be infinitely small. For n very large ('très-considérable'), the increase in $r_n(x)$ becomes 'insensible'. Therefore, the increase in $s(x)$ can only be an infinitely small quantity.

Cauchy's argument

est convergente, la somme de cette série est représentée par

$$u_0 + u_1 + u_2 + u_3 + \&c. \dots$$

En vertu de cette convention, la valeur du nombre ϵ se trouvera déterminée par l'équation

$$(6) \quad \epsilon = 1 + \frac{1}{1} + \frac{1}{1,2} + \frac{1}{1,2,3} + \frac{1}{1,2,3,4} + \&c. \dots;$$

et, si l'on considère la progression géométrique

$$1, x, x^2, x^3, \&c. \dots,$$

on aura, pour des valeurs numériques de x inférieures à l'unité,

$$(7) \quad 1 + x + x^2 + x^3 + \&c. \dots = \frac{1}{1-x}.$$

La série

$$u_0, u_1, u_2, u_3, \&c. \dots$$

étant supposée convergente, si l'on désigne sa somme par s , et par s_n la somme de ses n premiers termes, on trouvera

$$\begin{aligned} s &= u_0 + u_1 + u_2 + \dots + u_{n-1} + u_n + u_{n+1} + \&c. \dots \\ &= s_n + u_n + u_{n+1} + \&c. \dots, \end{aligned}$$

et par suite

$$s - s_n = u_n + u_{n+1} + \&c. \dots$$

De cette dernière équation il résulte que les quantités

$$u_n, u_{n+1}, u_{n+2}, \&c. \dots$$

formeront une nouvelle série convergente dont la somme sera équivalente à $s - s_n$. Si l'on représente cette même somme par r_n , on aura

$$s = s_n + r_n;$$

et r_n sera ce qu'on appelle le *reste* de la série (1) à partir du $n.$ ^{me} terme.

Lorsque, les termes de la série (1) renfermant une même variable x , cette série est convergente, et ses différents termes fonctions continues de x , dans le voisinage d'une valeur particulière attribuée à cette variable ;

$$s_n, r_n \text{ et } s$$

sont encore trois fonctions de la variable x , dont la première est évidemment continue par rapport à x dans le voisinage de la valeur particulière dont il s'agit. Cela posé, considérons les accroissements que reçoivent ces trois fonctions, lorsqu'on fait croître x d'une quantité infiniment petite α . L'accroissement de s_n sera, pour toutes les valeurs possibles de n , une quantité infiniment petite; et celui de r_n deviendra insensible en même temps que r_n , si l'on attribue à n une valeur très-considérable. Par suite, l'accroissement de la fonction s ne pourra être qu'une quantité infiniment petite. De cette remarque on déduit immédiatement la proposition suivante.

1.^{er} THÉORÈME. Lorsque les différents termes de la série (1) sont des fonctions d'une même variable x ,

A modern counterexample

For each $n \in \mathbb{N}$, define continuous functions f_n by

$$f_n(x) = \begin{cases} -1 & \text{if } x \leq -\frac{1}{n} \\ nx & \text{if } -\frac{1}{n} \leq x \leq \frac{1}{n} \\ +1 & \text{if } x \geq \frac{1}{n} \end{cases}$$

Now set $u_1(x) = f_1(x)$, and define new functions u_n recursively by

$$u_n(x) = f_n(x) - f_{n-1}(x)$$

Notice then that $s_n(x) = \sum_{j=1}^n u_j(x) = f_n(x)$

But we see that $s_n \rightarrow s$ as $n \rightarrow \infty$, where

$$s(x) = \begin{cases} -1 & \text{if } x < 0 \\ 0 & \text{if } x = 0 \\ +1 & \text{if } x > 0 \end{cases}$$

which is discontinuous at $x = 0$

A modern counterexample

What happens to the remainders $r_n(x) = s(x) - s_n(x)$?

Outside the range $-\frac{1}{n} \leq x \leq \frac{1}{n}$, $r_n(x) = 0$, but inside:

$$r_n(x) = \begin{cases} -1 - nx & \text{if } -\frac{1}{n} \leq x < 0 \\ 0 & \text{if } x = 0 \\ 1 - nx & \text{if } 0 < x \leq \frac{1}{n} \end{cases}$$

For each x , $r_n(x) \rightarrow 0$ as $n \rightarrow \infty$, but this does not happen **simultaneously** for all values of x

Cauchy's remainders

Cauchy: For n very large, the increase in $r_n(x)$ becomes 'insensible'. But what does this mean?

One of the following modern statements? (Denoting Cauchy's interval by I)

$$\forall \varepsilon > 0 : \exists N : \forall x \in I : n > N \Rightarrow |r_n(x)| < \varepsilon$$

$$\forall \varepsilon > 0 : \forall x \in I : \exists N : n > N \Rightarrow |r_n(x)| < \varepsilon$$

The second is true for our modern counterexample, but the first is not — so there really is a distinction between the two

Cauchy clearly didn't make this distinction

ϵ s and δ s



Karl Weierstrass (1815–1897)

Euclid's *Elements*

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

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

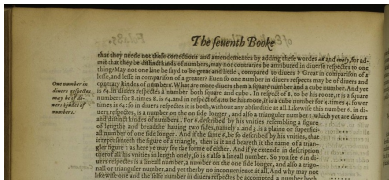
Book VI: similarity, proportion

Books VII–IX: number theory

Book X: commensurability, irrational numbers, surds

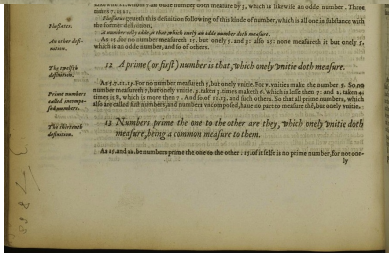
Books XI–XIII: solid geometry ending with the classification of the regular polyhedra

Euclid on prime numbers



12 A prime (or first) number is that, which onely vnitie doth measure.

As 5. 7. 11. 13. For no number measureth 5, but onely vnitie. For v. vnities make the number 5. So no
 number measureth 7, but onely vnitie. 2. taken 3. times maketh 6. which is lesse then 7: and 2, taken 4.
 times is 8, which is more then 7. And so of 11. 13. and such others. So that all prime numbers, which
 also are called first numbers, and numbers vncompounded, haue no part to measure the, but onely vnitie.



Euclid on prime numbers (Proposition IX.20)

of Euclides Elementes. 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 A 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 unto D . Wherefore A multiplieth E produced D , wherefore A mesureth D , but it also mesureth E not, which is impossible. Wherefore it is impossible to finde out a fourth number proportionall, with these numbers A, B, C , whensoever A mesureth not D .

But now suppose that A, B, C do not ether be continuall proportionall, neither also their extremes be as the one to the other. And let D be equal to C produce D . And in like sort 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. Theoreme. The 20. Proposition.

Prime numbers being given how many soever, there may be given a prime number.

Suppose that the prime numbers given be A, B, C . Then I say, that there yet more prime numbers besides A, B, C . Take (by the 31. of the seventh) a number whom these numbers A, B, C do measure, and let the same be E . And unto D, E adde unitie D, F . Now E, F is either a prime number or F is a prime number, then are there found these prime numbers A, B, C , and E, F more in multitude then the prime numbers first given A, B, C .

But now suppose that E, F be not prime. Wherefore some prime number mesureth it. (By the 24. of the seventh). Let a prime number measure it, namely, G . Then I say that G is none of these numbers A, B, C, F if G be one and the same with any of these A, B, C . But A, B, C measure the number D, E : and it also mesureth the whole E, F . Wherefore G being a number shall measure the residue D, F being unitie: 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 given A, B, C : which was required to be demonstrated.

¶ A Corollary.

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

¶ The 21. Theoreme. The 21. Proposition.

If ten numbers how many soever be added together: the whole shall be either prime or composite.

Prime numbers being given how many soever, there may be given more prime numbers.



Suppose that the prime numbers given be A, B, C . Then I say, that there are yet more prime numbers besides A, B, C . Take (by the 31. of the seventh) the least number whom these numbers A, B, C do measure, and let the same be D, E . And unto D, E adde unitie 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 given A, B, C .

But now suppose that E, F be not prime. Wherefore some prime number mesureth it (by the 24. of the seventh). Let a prime number measure it, namely, G . Then I say, that G is none of these numbers A, B, C, F if G be one and the same with any of these A, B, C . But A, B, C measure the number D, E : wherefore G also mesureth D, E : and it also mesureth the whole E, F . Wherefore G being a number shall measure the residue D, F being unitie: 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 given A, B, C : which was required to be demonstrated.

$A \dots$
 $B \dots$
 $C \dots$
 $E \ 114 \ D \cdot F$
 $G \dots$

Number theory after Euclid

Very little for many centuries...

Diophantus' *Arithmetica* (13 books, c. AD 250) featured number problems; for example:

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

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

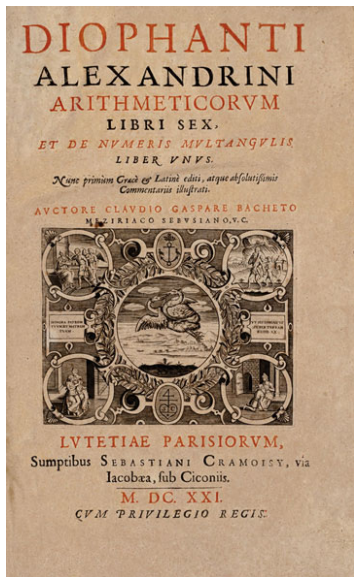
Sūnzǐ Suànjīng 孙子算经 (*The Mathematical Classic of Master Sun*) (3rd–5th century BC) contains a statement, but no proof, of the **Chinese Remainder Theorem** for the solution of simultaneous congruences

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** $x^2 - Dy^2 = 1$)

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 $a^p - a$

Conjectures on perfect numbers, and the search for Mersenne primes

Studies of Diophantine problems (more in a moment)

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

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 marvellous proof of this, which this margin is too narrow to contain.

17th-century attitudes to number theory

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

Pascal to Fermat (1655):

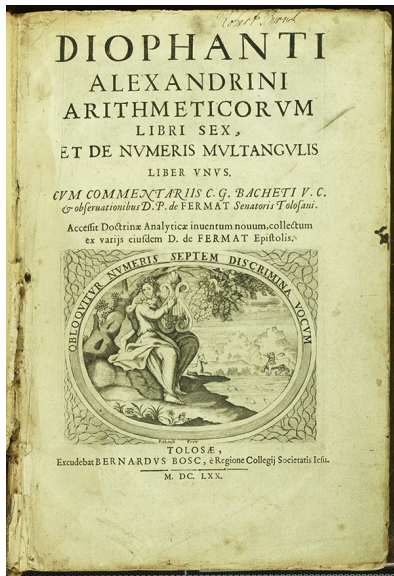
... seek elsewhere those who can follow you in your numerical discoveries ... I confess to you that this goes far beyond me ...

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. [...] Moreover, even if the proof of some proposition does not appear to have any present use, it usually turns out that the method by which this problem has been solved opens the way to the discovery of more useful results.

Euler on number theory

Euler (1747):

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. [...] Actually, far from being useless, this theory is of no little use even in analysis. 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 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 $\pi(x) \sim \frac{x}{\log x}, \dots$)

Fermat's Last Theorem in the 19th century

Many special cases have been proved by Euler and others in the 18th century . . .

Sophie Germain proved the theorem for certain classes of primes

Gabriel Lamé claimed to have proved the theorem by factorising $x^n + y^n = z^n$ in a cyclotomic field $\mathbb{Q}(\omega_n)$ — but he assumed that the cyclotomic integers $\mathbb{Z}(\omega_n)$ factorise uniquely (which they don't)

Ernst Eduard Kummer tried to fix this by introducing **ideal prime numbers** — new elements adjoined to the number field which facilitate unique factorisation

Fermat's Last Theorem in the 19th century

For Kummer, an 'ideal' was an extra element adjoined to a number field, assumed to have the same divisibility properties as the original elements

If an ideal element divides original elements a and b , then it also divides $a \pm b$ and all multiples of a and b . So Kummer's 'ideal' gives rise to a subset of original elements which it divides

Richard Dedekind, on the other hand, simply took this subset (in fact, a submodule) as his notion of 'ideal'

For a general algebraic number field, Dedekind showed that every ideal may be decomposed uniquely as a product of (suitably defined) 'prime' ideals

The result was the development of **ideal theory** by Dedekind, Wolfgang Krull, Emmy Noether, and others

The nature of the History of Mathematics

... mathematics [rarely] progresses only by means of 'great and significant works' and 'substantial changes'. [...] the truth is far more subtle and far more interesting: mathematics is the result of a cumulative endeavour to which many people have contributed, and not only through their successes but through half-formed thoughts, tentative proposals, partially worked solutions, and even outright failure. No part of mathematics came to birth in the form that it now appears in a modern textbook: mathematical creativity can be slow, sometimes messy, often frustrating.

Jacqueline A. Stedall, *From Cardano's great art to Lagrange's reflections: filling a gap in the history of algebra*, European Mathematical Society, 2011, p. ix