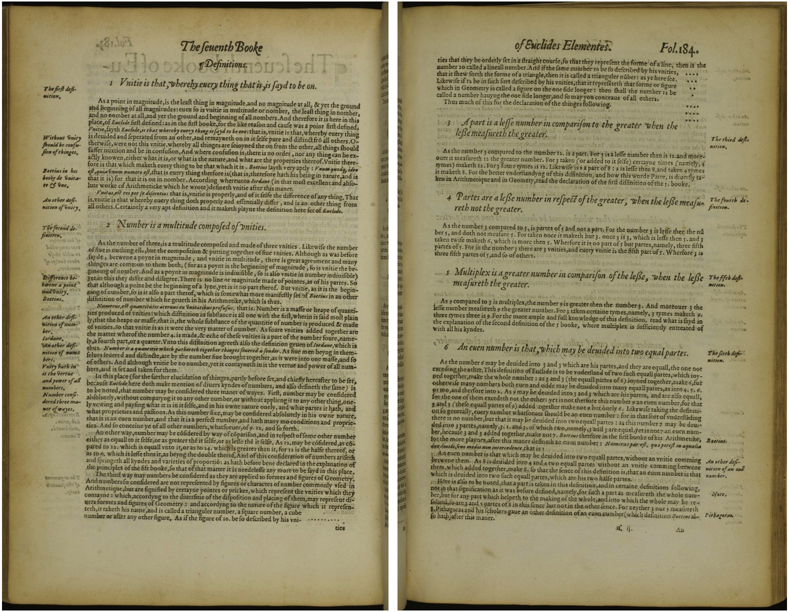
BO1 History of Mathematics
Lecture XV
Geometry and number theory
Part 2: Early number theory

MT 2020 Week 8

Euclid on numbers

Euclid on numbers (positive integers)

Euclid on numbers (positive integers)



¶ Definitions.

1 *Vnitie is that, whereby euery thing that is, is ſayd to be on.*

The firſt definition.

As a point in magnitude, is the leaſt thing in magnitude, and no magnitude at all, & yet the ground and beginning of all magnitudes: euen ſo is vnitie in multitude or nomber, the leaſt thing in nomber, and no nomber at all, and yet the ground and beginning of all nombers. And therefore it is here in this place, of *Euclide* firſt defined: as in the firſt booke, for the like reaſon and cauſe was a point firſt defined. *Vnitie*, ſayth *Euclide*, *is that whereby euery thing is ſayd to be one*: that is, vnitie is that, whereby euery thing is deuided and ſeperated from an other, and remayneth on in it ſelfe pure and diſtinct frō all others. Otherwiſe, were not this vnitie, whereby all thinges are ſeioyned the on from the other, all things ſhould ſuffer mixtion and be in confuſion. And where confuſion is, there is no order, nor any thing can be exactly knowen, either what it is, or what is the nature, and what are the properties thereof. Vnitie therefore is that which maketh euery thing to be that which it is. *Boetius* ſayth very aptly: *Vnum quodq; ideo eſt, quia vnum numero eſt*, that is euery thing therfore is (that is, therefore hath his being in nature, and is that it is) for that it is on in nomber. According whereunto *Iordane* (in that moſt excellent and abſolute worke of Arithmeticke which he wrote) defineth vnitie after this maner.

Without vnity ſhould be confuſion of thinges.

Boetius in his booke de vnitate & vno.

Vnitas, eſt rei per ſe diſcretio: that is, vnitie is properly, and of it ſelfe the difference of any thing. That is, vnitie is that whereby euery thing doth properly and eſſentially differ, and is an other thing from all others. Certainely a very apt definition and it maketh playne the definition here ſet of *Euclide*.

An other definition of vnity.

2 *Number is a multitude compoſed of vnities.*

The ſecond definition.

As the number of three, is a multitude compoſed and made of three vnities. Likewiſe the number of fiue is nothing elſe, but the compoſition & putting together of fiue vnities. Although as was before ſayde, betwene a poynt in magnitude, and vnitie in multitude, there is great agreement and many thinges are common to them both, (for as a poynt is the beginning of magnitude, ſo is vnitie the beginning of nomber. And as a poynt in magnitude is indiuiſible, ſo is alſo vnitie in number indiuiſible) yet in this they differ and diſagree. There is no line or magnitude made of pointes, as of his partes. So that although a point be the beginning of a lyne, yet is it no part therof. But vnitie, as it is the beginning of number, ſo is it alſo a part therof, which is ſomewhat more manifeſtly ſet of *Boetius* in an other diffinition of number which he geueth in his Arithmetike, which is thus.

Difference betwene a point and vnity. Boetius.

Numerus, eſt quantitatis aceruus ex vnitatibus profuſus, that is. Number is a maſſe or heape of quantities produced of vnities: which diffinition in ſubſtance is all one with the firſt, wherin is ſaid moſt plainly, that the heape or maſſe, that is, the whole ſubſtance of the quantitie of number is produced & made of vnities. So that vnitie is as it were the very matter of number. As foure vnities added together are the matter wherof the number 4. is made, & eche of theſe vnities is a part of the number foure, namely, a fourth part, or a quarter. Vnto this diffinition agreeth alſo the definition geuen of *Iordane*, which is thus. *Number is a quantitie which gathereth together thinges ſeuered a ſonder*. As fiue men beyng in themſelues ſeuered and diſtincte, are by the number fiue brought together, as it were into one maſſe, and ſo of others. And although vnitie be no number, yet it contayneth in it the vertue and power of all numbers, and is ſet and taken for them.

An other definition of number. Iordane. An other definition of number.

Vnity hath in it the vertue and power of all numbers.

In this place (for the farther elucidation of thinges, partly before ſet, and chiefly hereafter to be ſet, becauſe *Euclide* here doth make mention of diuers kyndes of numbers, and alſo defineth the ſame) is to be noted, that number may be conſidered three maner of wayes. Firſt, number may be conſidered abſolutely, without comparyng it to any other number, or without applieng it to any other thing, onely vewing and payſing what it is in it ſelfe, and in his owne nature onely, and what partes it hath, and what proprieties and paſſions. As this number ſixe, may be conſidered abſolutely in his owne nature, that it is an euen number, and that it is a perfect number, and hath many mo conditions and proprieties. And ſo conceiue ye of all other numbers, whatſoeuer, of 9. 12. and ſo forth.

Number conſidered three maner of wayes.

An other way, number may be cōſidered by way of cōpariſon, and in reſpect of ſome other number either as equall to it ſelfe, or as greater thē it ſelfe, or as leſſe thē it ſelfe. As 12. may be cōſidered, as cōpared to 12. which is equall vnto it, or as to 24. which is greater then it, for 12 is the halfe thereof, or as to 6. which is leſſe then it, as beyng the double therof. And of this conſideration of numbers ariſeth and ſpringeth all kyndes and varieties of proportiō: as hath before bene declared in the explanation of the principles of the fift booke, ſo that of that matter it is needeleſſe any more to be ſayd in this place.

The third way may numbers be conſidered as they are applied to formes and figures of Geometry. And numbers ſo conſidered are not repreſented by figures or charactes of number commonly vſed in Arithmetique, but are ſignified by certayne pointes or prickes, which repreſent the vnities which they contayne: which, accordyng to the diuerſitie of the diſpoſition and placing of them, may repreſent diuers formes and figures of Geometry: and accordyng to the nature of the figure which it repreſenteth, it taketh his name, and is called a trianguler number, a ſquare number, a cube number or after any other figure. As if the figure of 10. be ſo deſcribed by his vni- . . . .

ties

ties that they be orderly ſet in a ſtraight courſe, ſo that they repreſent the forme of a line, then is the number 10 called a lineall number. And if the ſame number 10 be ſo deſcribed by his vnities, that it ſhew forth the forme of a triangle, then it is called a trianguler nūber: as ye here ſee. Likewiſe if 12 be in ſuch ſort deſcribed by his vnities, that it repreſēteth that forme or figure which in Geometry is called a figure on the one ſide longer: then ſhall the number 12 be called a number hauyng the one ſide longer, and ſo may you conceaue of all others.

Thus much of this for the declaration of the thinges following.

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

The third definition.

As the number 3 compared to the number 12. is a part. For 3 is a leſſe number then is 12. and moreouer it meaſureth 12 the greater number. For 3 taken (or added to it ſelfe) certayne times (namely, 4 tymes) maketh 12. For 3 foure tymes is 12. Likewiſe is 2 a part of 8: 2 is leſſe then 8, and taken 4 tymes it maketh 8. For the better vnderſtandyng of this diffinition, and how this worde Parte, is diuerſly taken in Arithmetique and in Geometry, read the declaration of the firſt diffinition of the 5. booke.

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

The fourth definition.

As the number 3 compared to 5, is partes of 5 and not a part. For the number 3 is leſſe then the nūber 5, and doth not meaſure 5. For taken once it maketh but 3. once 3 is 3, which is leſſe then 5. and 3 taken twiſe maketh 6, which is more then 5. Wherfore it is no part of 5 but partes, namely, three fifth partes of 5. For in the number 3 there are 3 vnities, and euery vnitie is the fifth part of 5. Wherfore 3 is three fifth partes of 5, and ſo of others.

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

The fifth definition.

As 9 compared to 3 is multiplex, the number 9 is greater then the number 3. And moreouer 3 the leſſe number meaſureth 9 the greater number. For 3 taken certaine tymes, namely, 3 tymes maketh 9. three tymes three is 9. For the more ample and full knowledge of this definition, read what is ſayd in the explanation of the ſecond definition of the 5 booke, where multiplex is ſufficiently entreated of with all his kyndes.

6 *An euen number is that, which may be deuided into two equal partes.*

The ſixth definition.

As the number 6 may be deuided into 3 and 3 which are his partes, and they are equall, the one not exceding the other. This definition of Euclide is to be vnderſtand of two ſuch equall partes, which ioyned together, make the whole number: as 3 and 3 (the equall partes of 6) ioyned together, make 6, for otherwiſe many numbers both euen and odde may be deuided into many equall partes, as into 4. 5. 6. or mo, and therfore into 2. As 9 may be deuided into 3 and 3 which are his partes, and are alſo equall, for the one of them excedeth not the other: yet is not therfore this number 9 an euen number, for that 3 and 3 (theſe equall partes of 9) added together make not 9 but onely 6. Likewiſe taking the definition ſo generally, euery number whatſoeuer ſhould be an euen number: for in that ſort of vnderſtāding there is no number, but that it may be deuided into two equall partes: as this number 7 may be deuided into 3 partes, namely, 3. 1. and 3. of which two, namely, 3 and 3 are equal, yet is not 7 an euen number, becauſe 3 and 3 added together, make not 7. *Boetius* therfore in the firſt booke of his Arithmetike, for the more playnes, after this maner defineth an euen number: *Numerus par eſt, qui poteſt in aequalia duo diuidi, vno medio non intercedente*, that is:

Boetius.

An euen number is that which may be deuided into two equall partes, without an vnitie comming betwene them. As 8 is deuided into 4 and 4 two equall partes without an vnitie comming betwene them, which added together, make 8, ſo that the ſence of this definition is, that an euen number is that which is deuided into two ſuch equall partes, which are his two halfe partes.

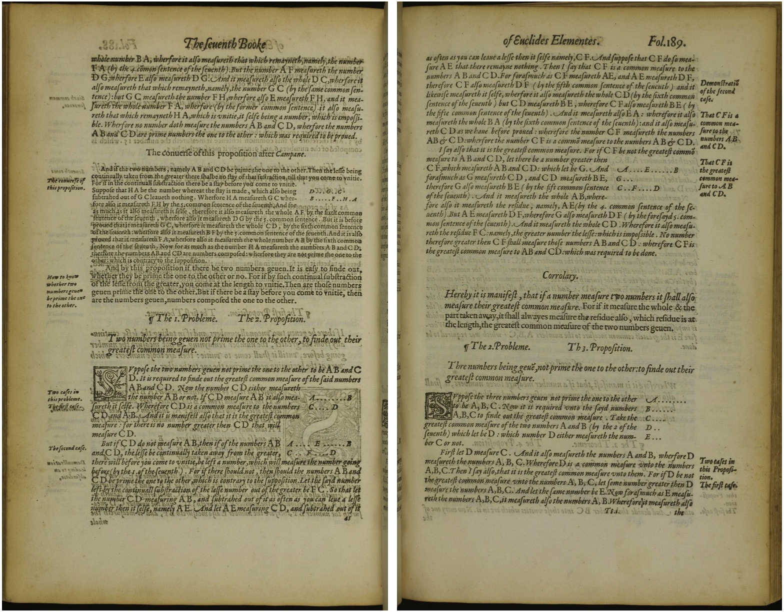
An other definition of an euē number.

Here is alſo to be noted, that a part is taken in this definition, and in certaine definitions following, not in that ſignification as it was before defined, namely, for ſuch a part as meaſureth the whole number, but for any part which helpeth to the making of the whole, and into which the whole may be reſolued, ſo are 3 and 5 partes of 8 in this ſence but not in the other ſence. For neyther 3 nor 5 meaſureth 8. Pithagoras and his ſcholers gaue an other definition of an euen number (which definition *Boetius* alſo hath) after this maner.

Note.

Pithagoras.

The Euclidean algorithm (Proposition VII.2)



whole number B A, wherfore it also measureth that which remayneth, namely, the number F A (by the 4. cōmon sentence of the seuenth). But the number A F measureth the number D G, wherfore E also measureth D G. And it measureth also the whole D C, wherfore it also measureth that which remayneth, namely, the number G C (by the same common sentence): but G C measureth the number F H, wherfore also E measureth F H, and it measureth the whole number F A, wherfore (by the former common sentence) it also measureth that which remayneth H A, which is vnitie, it selfe being a number, which is impossible. Wherfore no number doth measure the numbers A B and C D, wherfore the numbers A B and C D are prime numbers the one to the other: which was required to be proued.

The conuerse of this proposition after *Campane*.

The conuerse of this proposition.

And if the two numbers, namely A B and C D be prime the one to the other. Then the lesse being continually taken from the greater there shalbe no stay of that sustraction, till that you come to vnitie. For if in the continuall substraction there be a stay before you come to vnitie. Suppose that H A be the number whereat the stay is made, which also being subtrahed out of G C leaueth nothing. Wherfore H A measureth G C wherfore also it measureth F H by the 5. common sentence of the seuenth. And for as much as it also measureth it selfe, therefore it also measureth the whole A F by the sixth common sentence of the seuenth, wherfore also it measureth D G by the 5. common sentence. But it is before proued that it measureth G C, wherfore it measureth the whole C D, by the sixth common sentence of the seuenth: wherfore also it measureth B F by the 5. common sentence of the seuenth. And it is also proued that it measureth F A, wherfore also it measureth the whole number A B by the sixth common sentence of the seuenth, Now for as much as the number H A measureth the numbers A B and C D, therfore the numbers AB and CD are numbers composed: wherfore they are not prime the one to the other: which is contrary to the supposition.

D . . . G . . C
B . . . . . F . . H . A

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

And by this proposition if there be two numbers geuen. It is easy to finde out, whether they be prime the one to the other or no. For if by such continual substraction of the lesse from the greater, you come at the length to vnitie. Then are those numbers geuen prime the one to the other. But if there be a stay before you come to vnitie, then are the numbers geuen, numbers composed the one to the other.

¶ The 1. Probleme. The 2. Proposition.

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

Two cases in this probleme. The first case.

Suppose the two numbers geuen not prime the one to the other to be A B *and* C D. *It is required to finde out the greatest common measure of the said numbers* A B *and* C D. *Now the number* C D *either measureth the number* A B *or not. If* C D *measure* A B *it also measureth it selfe. Wherefore* C D *is a common measure to the numbers* C D *and* A B. *And it is manifest also that it is the greatest common measure: for there is no number greater then* C D *that will measure* C D.

A . . . . B
C . . . . D

The second case.

But if C D *do not measure* A B, *then if of the numbers* A B *and* C D, *the lesse be continually taken away from the greater, there will before you come to vnitie, be left a number, which will measure the number going before (by the 1. of the seuenth). For if there should not, then should the numbers* A B *and* C D *be prime the one to the other, which is contrary to the supposition. Let the sayd number left by the continuall substraction of the lesse number out of the greater be* F C. *So that let the number* C D *measuring* A B, *and subtrahed out of it as often as you can leue a lesse number then it selfe, namely* A E. *And let* A E *measuring* C D, *and subtrahed out of it*

A . . . . E . . . . . . B
C . . F . . . . D

as often as you can leaue a lesse then it selfe namely, C F. *And suppose that* C F *do so measure* A E *that there remayne nothing. Then I say that* C F *is a common measure to the numbers* A B *and* C D. *For forasmuch as* C F *measureth* AE, *and* A E *measureth* D F, *therefore* C F *also measureth* D F *(by the fifth common sentence of the seuenth) and it likewise measureth it selfe, wherfore it also measureth the whole* C D *(by the sixth common sentence of the seuenth) but* C D *measureth* B E, *wherefore* C F *also measureth* B E *(by the fifte common sentence of the seuenth). And it measureth also* E A: *wherefore it also measureth the whole* B A *(by the sixth common sentence of the seuenth): and it also measureth* C D *as we haue before proued: wherefore the number* C F *measureth the numbers* AB & C D: *wherfore the number* C F *is a cōmō measure to the numbers* A B & C D.

Demonstratiō of the second case.

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

I say also that it is the greatest common measure. For if C F *be not the greatest cōmō measure to* A B *and* C D, *let there be a number greater then* C F, *which measureth* A B *and* C D: *which let be* G. *And forasmuch as* G *measureth* C D, *and* C D *measureth* B E, *therefore* G *also measureth* B E *(by the fift common sentence of the seuenth). And it measureth the whole* A B, *wherefore also it measureth the residue, namely,* A E *(by the 4. common sentence of the seuenth). But* A E *measureth* D F, *wherefore* G *also measureth* D F *(by the foresayd 5. common sentence of the seuenth). And it measureth the whole* C D. *Wherefore it also measureth the residue* F C: *namely, the greater number the lesse: which is impossible. No number therefore greater then* C F *shall measure those numbers* A B *and* C D: *wherefore* C F *is the greatest common measure to* AB *and* CD: *which was required to be done.*

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

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

Corrolary.

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 alwayes measure the residue also, which residue is at the length, the greatest common measure of the two numbers geuen.

¶ The 2. Probleme. Th 3. Proposition.

Thre numbers being geuē, not prime the one to the other: to finde out their greatest common measure.

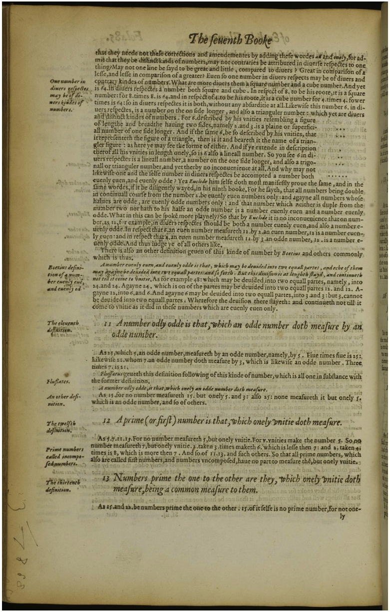
Suppose the three numbers geuen not prime the one to the other to be A, B, C. *Now it is required vnto the sayd numbers* A, B, C *to finde out the greatest common measure. Take the greatest common measure of the two numbers* A *and* B *(by the 2 of the seuenth) which let be* D: *which number* D *either measureth the number* C *or not.*

A . . . .
B . . . . . .
C . . . .
D . .
E . . .

Two cases in this Proposition. The first case.

First let D *measure* C. *And it also measureth the numbers* A *and* B, *wherfore* D *measureth the numbers* A, B, C. *Wherefore* D *is a common measure vnto the numbers* A, B, C. *Then I say also, that it is the greatest common measure vnto them. For if* D *be not the greatest common measure vnto 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 forasmuch as* E *measureth the numbers* A, B, C, *it measureth also the numbers* A, B. *Wherefore it measureth also the*

Euclid on prime numbers



The seuenth Booke

that they neede not these corrections and amendementes by adding these wordes *all* and *onely*, for admit that they be distinct kinds of numbers, may not contraries be attributed in diuerse respectes to one thing? May not one line be sayd to be great and little, compared to diuers? Great in comparison of a lesse, and lesse in comparison of a greater? Euen so one number in diuers respects may be of diuers and contrary kindes of numbers. What are more diuers them a square number and a cube number. And yet is 64. in diuers respectes a number both square and cube. In respect of 8. to be his roote, it is a square number: for 8. times 8. is 64. and in respect of 4. to be his roote, it is a cube number for 4. times 4. fower times is 64: so in diuers respectes it is both, without any absurditie at all. Likewise this number 6. in diuers respectes, is a number on the on side longer, and also a trianguler number: which yet are diuers and distinct kindes of numbers. For 6. described by his vnities resembling a figure of lengthe and breadthe hauing two sides, namely 2. and 3. is a plaine or superficiall number of one side longer. And if the same 6, be so described by his vnities, that it representeth the figure of a triangle, then is it and beareth it the name of a triangler figure: as here ye may see the forme of either. And if ye extende in description therof all his vnities in length onely, so is 6 also a lineall number. So you see 6 in diuers respectes is a lineall number, a number on the one side longer, and also a trigonall or trianguler number, and yet therby no inconuenience at all. And why may not likewise one and the selfe number in diuers respectes be accompted a number both euenly euen, and euenly odde? Yea *Euclide* him selfe doth most manifestly proue the same, and in the same wordes, if it be diligently wayed, in his ninth booke. For he sayth, that all numbers being double in continuall course from the number 2. be euenly euen numbers only: and agayne all numbers whose halues are odde, are euenly odde numbers only: and that number which neither is duple from the number two nor hath to his halfe an odde number is a number euenly euen and a number euenly odde. What in this can be spokē more playnely? So that by *Euclide* it is no inconuenience that on number, as 12, for example, in diuers respectes should be both a number euenly euen, and also a number euenly odde. In respect that 6. an euen number measureth 12. by 2. an euen number, 12 is a number euenly euen: and in respect that 4. an euen number measureth 12. by 3. an odde number, 12. is a number euenly odde. And thus iudge ye of all others like.

One number in diuers respectes may be of diuers kindes of numbers.

There is also an other definition geuen of this kinde of number by *Boetius* and others commonly which is thus.

A number euenly euen, and euenly odde is that, which may be deuided into two equall partes, and eche of them may agayne be deuided into two equall partes: and so forth. But this diuision is at lenghth stayd, and continueth not till it come to vnitie. As for example 48: which may be deuided into two equall partes, namely, into 24. and 24. Agayne 24. which is on of the partes may be deuided into two equall partes 12. and 12. Agayne 12, into 6. and 6. And agayne 6 may be deuided into two equall partes, into 3. and 3: but 3. cannot be deuided into two equall partes. Wherefore the deuision there stayeth: and continueth not till it come to vnitie as it did in these numbers which are euenly euen only.

Boetius definition of a number euenly euē, and euenly od.

The eleuenth definition.

11 *A number odly odde is that, which an odde number doth measure by an odde number.*

As 25, which 5. an odde number, measureth by an odde number, namely, by 5. Fiue times fiue is 25: Likewise 21. whom 7. an odde number doth measure by 3, which is likewise an odde number. Three times 7. is 21.

Flussatus geueth this definition following of this kinde of number, which is all one in substance with the former definition.

Flussates.

A number odly odde, is that, which onely an odde number doth measure.

As 15. for no number measureth 15. but onely 5. and 3: also 25: none measureth it but onely 5. which is an odde number, and so of others.

An other definition.

The twelfth definition.

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 vncomposed, haue no part to measure thē, but onely vnitie.

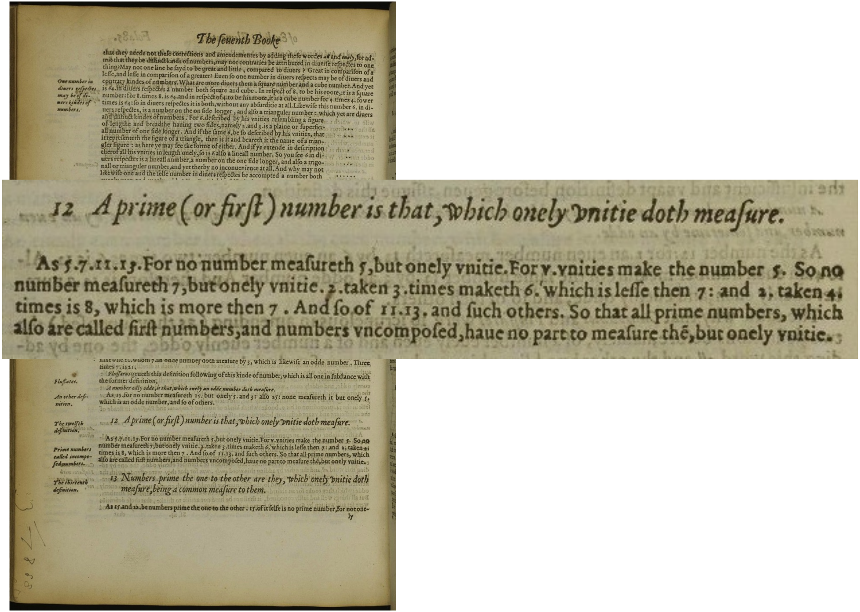
Prime numbers called incomposed numbers.

The thirtenth definition.

13 *Numbers prime the one to the other are they, which onely vnitie doth measure, being a common measure to them.*

As 15. and 22. be numbers prime the one to the other. 15. of it selfe is no prime number, for not onely

Euclid on prime numbers



The seuenth Booke

that they neede not these corrections and amendementes by adding these wordes *all* and *onely*, for admit that they be distinct kinds of numbers, may not contraries be attributed in diuerse respectes to one thing? May not one line be sayd to be great and little, compared to diuers? Great in comparison of a lesse, and lesse in comparison of a greater? Euen so one number in diuers respects may be of diuers and contrary kindes of numbers. What are more diuers them a square number and a cube number. And yet is 64. in diuers respectes a number both square and cube. In respect of 8. to be his roote, it is a square number: for 8. times 8. is 64. and in respect of 4. to be his roote, it is a cube number for 4. times 4. fower times is 64: so in diuers respectes it is both, without any absurditie at all. Likewise this number 6. in diuers respectes, is a number on the on side longer, and also a trianguler number: which yet are diuers and distinct kindes of numbers. For 6. described by his vnities resembling a figure of lengthe and breadthe hauing two sides, namely 2. and 3. is a plaine or superficiall number of one side longer. And if the same 6, be so described by his vnities, that it representeth the figure of a triangle, then is it and beareth it the name of a triangler figure: as here ye may see the forme of either. And if ye extende in description therof all his vnities in length onely, so is 6 also a lineall number. So you see 6 in diuers respectes is a lineall number, a number on the one side longer, and also a trigonall or trianguler number, and yet therby no inconuenience at all. And why may not likewise one and the selfe number in diuers respectes be accompted a number both

One number in diuers respectes may be of diuers kindes of 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 vncomposed, haue no part to measure thē, but onely vnitie.

likewise 21. whom 7. an odde number doth measure by 3, which is likewise an odde number. Three times 7. is 21.

Flussatus geueth this definition following of this kinde of number, which is all one in substance with the former definition.

A number odly odde, is that, which onely an odde number doth measure.

As 15. for no number measureth 15. but onely 5. and 3: also 25: none measureth it but onely 5. which is an odde number, and so of others.

Flussates.

An other definition.

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 vncomposed, haue no part to measure thē, but onely vnitie.

The twelfth definition.

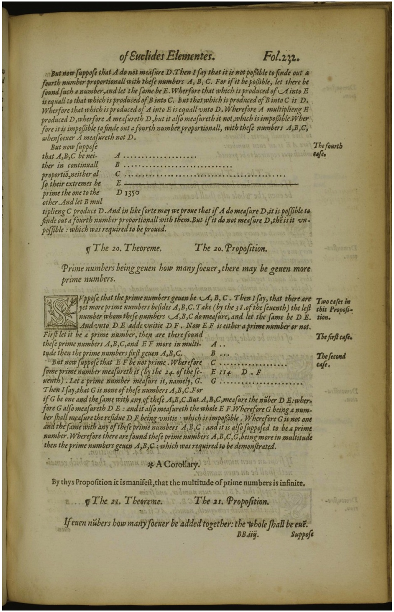
Prime numbers called incomposed numbers.

13 *Numbers prime the one to the other are they, which onely vnitie doth measure, being a common measure to them.*

The thirtenth definition.

As 15. and 22. be numbers prime the one to the other. 15. of it selfe is no prime number, for not onely

Euclid on prime numbers (Proposition IX.20)



of Euclides Elementes. Fol.232.

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. Wherfore that which is produced of A into E is equall to that which is produced of B into C. But that which is produced of B into C is D. Wherfore that which is produced of A into E is equall vnto D. Wherefore A multiplieng E produced D, wherfore A meaſureth D, but it alſo meaſureth it not, which is impoſsible. Wherfore it is impoſsible to finde out a fourth number proportionall, with theſe numbers A,B,C, whenſoeuer A meaſureth not D.

The fourth caſe.

But now ſuppoſe that A,B,C be neither in continuall proportiō, neither alſo their extremes be prime the one to the other. And let B multiplieng C produce D. And in like ſorte may we proue 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, thē is it vnpoſsible: which was required to be proued.

A ....
B ....
C ....
E
D 1350

¶ The 20. Theoreme. The 20. Propoſition.

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

Two caſes in this Propoſition.

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 ſeuenth) the leſt number whom theſe numbers A,B,C do meaſure, and let the ſame be D E. And vnto D E adde vnitie D F. Now E F is either a prime number or not.

The first caſe.

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.

The ſecond caſe.

But now ſuppoſe that E F be not prime. Wherefore ſome prime number meaſureth it (by the 24. of the ſeuenth). 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 nūber D E: wherfore 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 vnitie: which is impoſsible. Wherefore G is not one and the ſame with any of theſe prime numbers A,B,C: and it is alſo ſuppoſed to be a prime number. Wherefore there are found theſe prime numbers A,B,C,G, being more in multitude then the prime numbers geuen A,B,C: which was required to be demonſtrated.

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

A Corollary.

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

¶ The 21. Theoreme. The 21. Propoſition.

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

BB.iiij. Suppoſe

Euclid on prime numbers (Proposition IX.20)

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. Wherfore that which is produced of A into E is equall to that which is produced of B into C. But that which is produced of B into C is D. Wherfore that which is produced of A into E is equall vnto D. Wherefore A multiplieng E produced D, wherfore A meaſureth D, but it alſo meaſureth it not, which is impoßible. Wherfore it is impoßible to finde out a fourth number proportionall, with theſe numbers A, B, C whenſoeuer A meaſureth not D.

But now ſuppoſe that A, B, C be neither in continuall proportiõ, neither alſo their extremes be prime the one to the other. And let B multiplieng C produce D. And in like ſorte may we proue 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, thẽ is it impoſſible: which was required to be proued.

A ....

B ....

C ....

E ————————————————

D 1350

¶ The 20. Theoreme. The 20. Propoſition.

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

Vppoſe 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 ſeuenth) the leſt number whom theſe numbers A, B, C do meaſure, and let the ſame be D E. And vnto D E adde vnitie 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 ſeuenth). 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 nũber D E: wherfore 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 vnitie: which is impoßible. Wherefore G is not one and the ſame with any of theſe prime numbers A, B, C: and it is alſo ſuppoſed to be a prime number. Wherefore there are found theſe prime numbers A, B, C, G, being more in multitude then the prime numbers geuen A, B, C: which was required to be demonſtrated.

A ..

B ...

C ....

E 114 D . F

G ....

✻ A Corollary.

By thys Propoſition it is manifeſt, that the multitude of prime numbers is infini...

¶ The 21. Theoreme. The 21. Propoſition.

If euen nũbers how many ſoeuer be added together: the whole ſhall be euẽ.

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

Vppoſe 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 ſeuenth) the leſt number whom theſe numbers A, B, C do meaſure, and let the ſame be D E. And vnto D E adde vnitie 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 ſeuenth). 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 nũber D E: wherfore 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 vnitie: which is impoßible. Wherefore G is not one and the ſame with any of theſe prime numbers A, B, C: and it is alſo ſuppoſed to be a prime number. Wherefore there are found theſe prime numbers A, B, C, G, being more in multitude then the prime numbers geuen A, B, C: which was required to be demonſtrated.

A ..

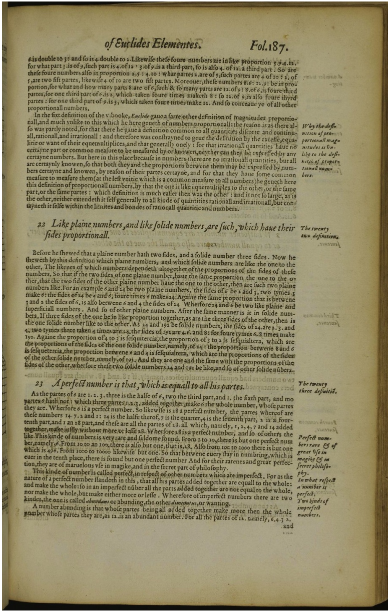
B ...

C ....

E 114 D . F

G ....

Euclid on perfect numbers



6.is double to 3: and so is 4.double to 2. Likewise these foure numbers are in like proportion 3.9.4.12. for what part 3.is of 9, such part is 4.of 12 · 3.of 9.is a third part, so is also 4. of 12. a third part. So are these foure numbers also in proportion 2.5 : 4.10 : what partes 2.are of 5, such partes are 4.of 10 : 2, of 5, are two fift partes, likewise 4.of 10 are two fift partes. Moreouer, these numbers 8.6: 12.9: be in proportion, for what and how many parts 8.are of 6, such & so many parts are 12.of 9: 8.of 6, is foure third partes, for one third part of 6.is 2, which taken foure times maketh 8 : so 12.of 9, is also foure thyrd partes : for one third part of 9.is 3, which taken foure times make 12. And so conceaue ye of all other proportionall numbers.

In the sixt definition of the v.booke, *Euclide* gaue a farre other definition of magnitudes proportionall, and much vnlike to this which he here geueth of numbers proportionall: the reason is as there also was partly noted, for that there he gaue a definition common to all quantities discrete and continuall, rationall, and irrationall : and therefore was constrayned to geue the definition by the excesse, equalitie or want of their equemultiplices, and that generally onely : for that irrationall quantities haue no certayne part or common measure to be measured by or knowen, neyther can they be expressed by any certayne numbers. But here in this place because in numbers there are no irrationall quantities, but all are certaynly knowen, so that both they and the proportions betwene them may be expressed by numbers certayne and knowen, by reason of their partes certayne, and for that they haue some common measure to measure them (at the lest vnitie which is a common measure to all numbers) he geueth here this definition of proportionall numbers, by that the one is like equemultiplex to the other, or the same part, or the same partes : which definition is much easier then was the other : and is not so large, as is the other, neither extendeth it self generally to all kinde of quantities rationall and irrationall, but conteyneth it selfe within the limites and bondes of rationall quantitie and numbers. *Why the definition of proportionall magnitudes is vnlike to the definition of proportionall numbers.*

22 *Like plaine numbers, and like solide numbers, are such, which haue their sides proportionall.* *The twenty two definition.*

Before he shewed that a plaine number hath two sides, and a solide number three sides. Now he sheweth by this definition which plaine numbers, and which solide numbers are like the one to the other. The likenes of which numbers dependeth altogether of the proportions of the sides of these numbers. So that if the two sides of one plaine number, haue the same proportion the one to the other, that the two sides of the other plaine number haue the one to the other, then are such two plaine numbers like. For an example 6 and 24 be two plaine numbers, the sides of 6 be 2 and 3, two tymes 3 make 6: the sides of 24 be 4 and 6, foure times 6 makes 24. Againe the same proportion that is betwene 3 and 2 the sides of 6. is also betwene 6 and 4 the sides of 24 Wherfore 24 and 6 be two like plaine and superficiall numbers. And so of other plaine numbers. After the same manner is it in solide numbers. If three sides of the one be in like proportion together, as are the three sides of the other, then is the one solide number like to the other. As 24 and 192 be solide numbers, the sides of 24.are 2. 3. and 4, two tymes three taken 4 times are 24. the sides of 192 are 4.6. and 8: for foure tymes 6. 8 times make 192. Againe the proportion of 4 to 3 is sesquitercia, the proportion of 3 to 2 is sesquialtera, which are the proportions of the sides of the one solide number, namely, of 24 : the proportion betwene 8 and 6 is sesquetercia, the proportion betwene 6 and 4 is sesquialtera, which are the proportions of the sides of the other solide number, namely, of 192. And they are one and the same with the proportions of the sides of the other, wherfore these two solide numbers 24 and 192 be like, and so of other solide nũbers.

23 *A perfect number is that, which is equall to all his partes.* *The twenty three definitiõ.*

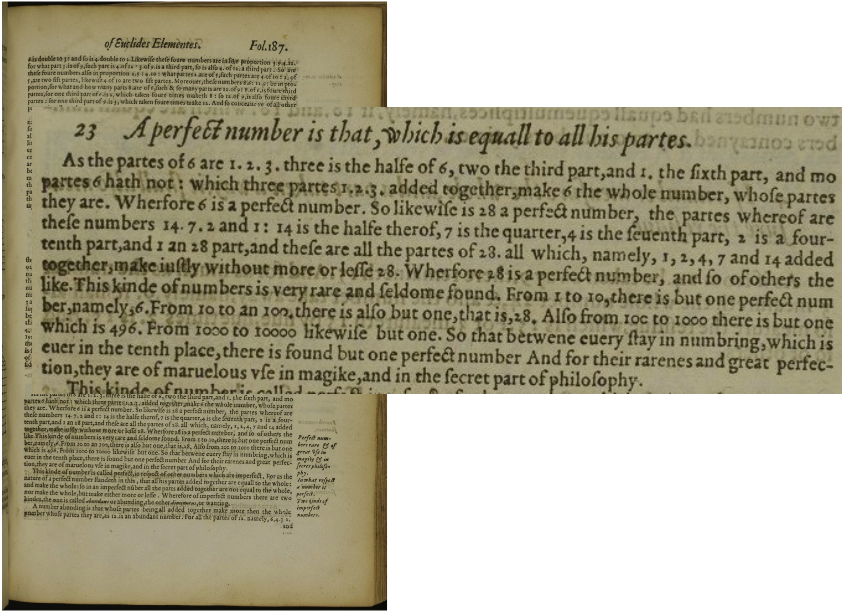
As the partes of 6 are 1. 2. 3. three is the halfe of 6, two the third part, and 1. the sixth part, and mo partes 6 hath not : which three partes 1.2.3. added together, make 6 the whole number, whose partes they are. Wherfore 6 is a perfect number. So likewise is 28 a perfect number, the partes whereof are these numbers 14. 7. 2 and 1: 14 is the halfe therof, 7 is the quarter, 4 is the seuenth part, 2 is a fourtenth 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. Wherfore 28 is a perfect number, and so of others 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 euery 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. *Perfect numbers rare & of great vse in magike & in secret philosophy.*

This kinde of number is called perfect, in respect of other numbers which are imperfect. For as the nature of a perfect number standeth in this, that all his partes added together are equall to the whole: and make the whole: so in an imperfect nũber all the parts added together are not equal to the whole, nor make the whole, but make either more or lesse. Wherefore of imperfect numbers there are two kindes, the one is called *abundans* or abunding, the other *diminutus*, or wanting. *In what respect a number is perfect.* *Two kindes of imperfect numbers.*

A number abunding is that whose 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, 6, 4, 3, 2,

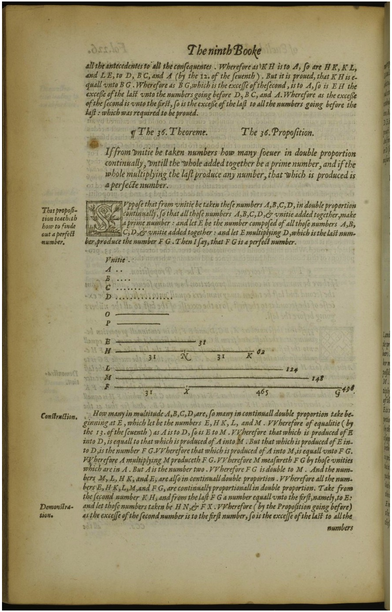
and

Euclid on perfect numbers


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. Wherfore 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 seuenth part, 2 is a fourtenth 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. Wherfore 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 euery 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.

Euclid on perfect numbers (Proposition IX.36)



The ninth Booke

all the antecedentes to all the consequentes. Wherefore as K H is to A, so are H K, K L, and L E, to D, B C, and A (by the 12. of the seuenth). But it is proued, that K H is equall vnto B G. Wherefore as B G, which is the excesse of the second, is to A, so is E H the excesse of the last vnto the numbers going before D, B C, and A. Wherefore as the excesse of the second is vnto the first, so is the excesse of the last to all the numbers going before the last: which was required to be proued.

¶ The 36. Theoreme. The 36. Proposition.

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.

This proposition teacheth how to finde out a perfect number.

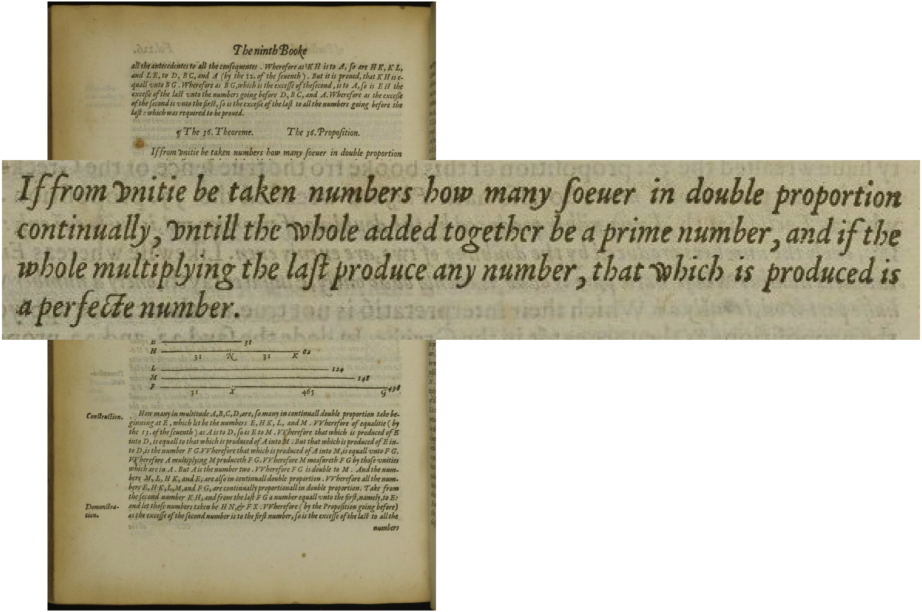
Suppose that from vnitie be taken these numbers A, B, C, D, in double proportion continually, so that all those numbers A, B, C, D, & vnitie added together, make a prime number: and let E be the number composed of all those numbers A, B, C, D, & vnitie added together: and let E multiplying D, which is the last number, produce the number F G. Then I say, that F G is a perfect number.

Construction. How many in multitude A, B, C, D, are, so many in continuall double proportion take beginning at E, which let be the numbers E, H K, L, and M. VVherefore of equalitie (by the 13. of the seuenth) as A is to D, so is E to M. VVherefore that which is produced of E into D, is equall to that which is produced of A into M. But that which is produced of E into D, is the number F G. VVherefore that which is produced of A into M, is equall vnto F G. VVherefore A multiplying M produceth F G. VVherefore M measureth F G by those vnities which are in A. But A is the number two. VVherefore F G is double to M. And the numbers M, L, H K, and E, are also in continuall double proportion. VVherefore all the numbers E, H K, L, M, and F G, are continually proportionall in double proportion. Take from the second number K H, and from the last F G a number equall vnto the first, namely, to E: and let those numbers taken be H N, & F X. VVherefore (by the Proposition going before) as the excesse of the second number is to the first number, so is the excesse of the last to all the

Demonstration.

numbers

Euclid on perfect numbers (Proposition IX.36)



The ninth Booke

all the antecedentes to all the consequentes. Wherefore as KH is to A, so are HK, KL, and LE, to D, BC, and A (by the 12. of the seuenth). But it is proued, that KH is equall vnto BG. Wherefore as BG, which is the excesse of the second, is to A, so is EH the excesse of the last vnto the numbers going before D, BC, and A. Wherefore as the excesse of the second is vnto the first, so is the excesse of the last to all the numbers going before the last: which was required to be proued.

¶ The 36. Theoreme. The 36. Proposition.

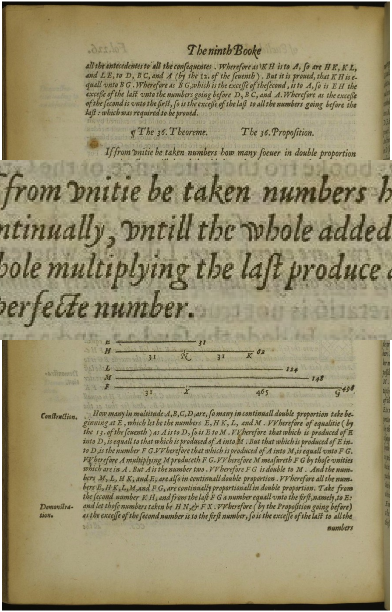
If from vnitie be taken numbers how many soeuer in double proportion continually, vntill the whole added together be a prime number, and if the whole multiplying the last produce any number, that which is produced is a perfecte number.

Construction. How many in multitude A, B, C, D, are, so many in continuall double proportion take beginning at E, which let be the numbers E, HK, L, and M. VVherefore of equalitie (by the 13. of the seuenth) as A is to D, so is E to M. VVherefore that which is produced of E into D, is equall to that which is produced of A into M. But that which is produced of E into D, is the number FG. VVherefore that which is produced of A into M, is equall vnto FG. VVherefore A multiplying M produceth FG. VVherefore M measureth FG by those vnities which are in A. But A is the number two. VVherefore FG is double to M. And the numbers M, L, HK, and E, are also in continuall double proportion. VVherefore all the numbers E, HK, L, M, and FG, are continually proportionall in double proportion. Take from the second number KH, and from the last FG a number equall vnto the first, namely, to E: and let those numbers taken be HN, & FX. VVherefore (by the Proposition going before) as the excesse of the second number is to the first number, so is the excesse of the last to all the

Demonstration.

numbers

Euclid on perfect numbers (Proposition IX.36)



The ninth Booke

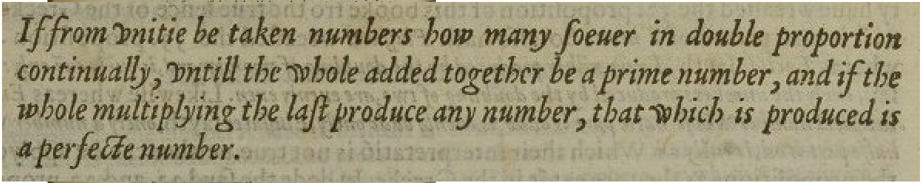
all the antecedentes to all the consequentes. Wherefore as KH is to A, so are HK, KL, and LE, to D, BC, and A (by the 12. of the seuenth). But it is proued, that KH is equall vnto BG. Wherefore as BG, which is the excesse of the second, is to A, so is EH the excesse of the last vnto the numbers going before D, BC, and A. Wherefore as the excesse of the second is vnto the first, so is the excesse of the last to all the numbers going before the last: which was required to be proued.

¶ The 36. Theoreme. The 36. Proposition.

If from vnitie be taken numbers how many soeuer in double proportion

Construction. How many in multitude A, B, C, D, are, so many in continuall double proportion take beginning at E, which let be the numbers E, HK, L, and M. VVherefore of equalitie (by the 13. of the seuenth) as A is to D, so is E to M. VVherefore that which is produced of E into D, is equall to that which is produced of A into M. But that which is produced of E into D, is the number FG. VVherefore that which is produced of A into M, is equall vnto FG. VVherefore A multiplying M produceth FG. VVherefore M measureth FG by those vnities which are in A. But A is the number two. VVherefore FG is double to M. And the numbers M, L, HK, and E, are also in continuall double proportion. VVherefore all the numbers E, HK, L, M, and FG, are continually proportionall in double proportion. Take from the second number KH, and from the last FG a number equall vnto the first, namely, to E: and let those numbers taken be HN, & FX. VVherefore (by the Proposition going before)

Demonstration. as the excesse of the second number is to the first number, so is the excesse of the last to all the numbers



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...

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 IX]:

> 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 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;

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*

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*

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

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

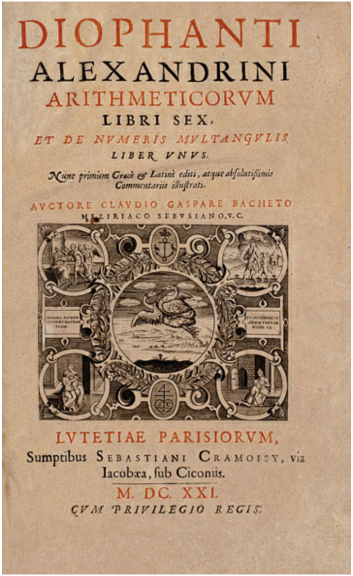
Sūnzǐ Suànjīng 孙子算经 (*The Mathematical Classic of Master Sun*) (3rd–5th century BC) contains a statement, but no proof, of the Chinese Remainder Theorem for the solution of simultaneous congruences

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

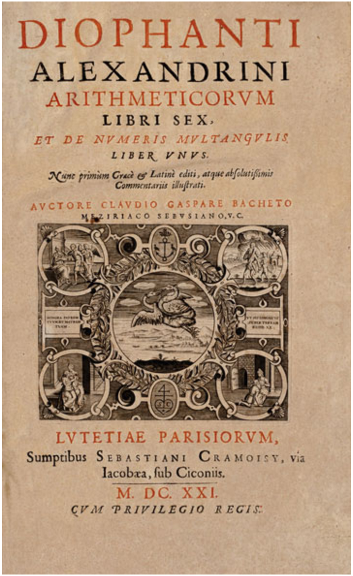
17th-century number theory



DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO MEZIRIACO SEBVSIANO, V.C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

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

17th-century number theory


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis
Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via
Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

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 $a^p - a$

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 $p \le 257$ 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):

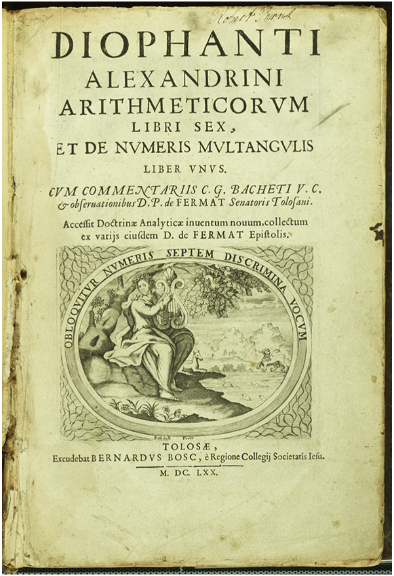
> *... seek elsewhere those who can follow you in your numerical discoveries ... I confess to you that this goes far beyond me ...*

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



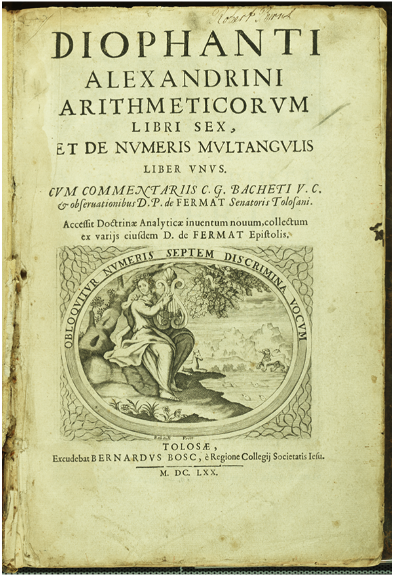
DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& obſeruationibus D. P. de FERMAT *Senatoris Toloſani.*
Acceſſit Doctrinæ Analyticæ inuentum nouum, collectum
ex varijs eiuſdem D. de FERMAT Epiſtolis.

NVMERIS SEPTEM DISCRIMINA VOCVM OBLOQVITVR

TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Ieſu.
M. DC. LXX.

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

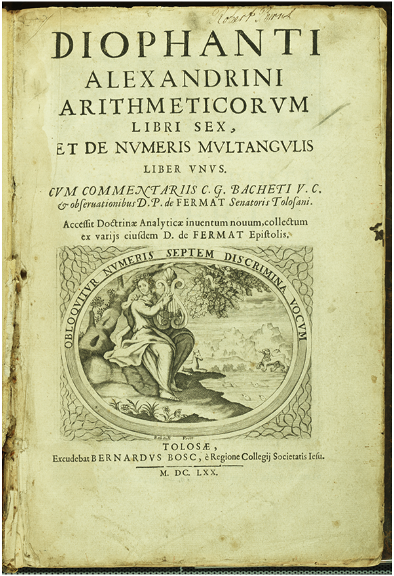
The 'rebirth' of number theory



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


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& obseruationibus D. P. de FERMAT Senatoris Tolosani.
Accessit Doctrinæ Analyticæ inuentum nouum, collectum ex varijs eiusdem D. de FERMAT Epistolis.
OBLOQVITVR NVMERIS SEPTEM DISCRIMINA VOCVM
TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Iesu.
M. DC. LXX.

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

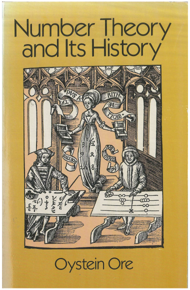
19th-century number theory

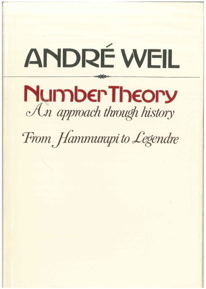
Gauss's *Disquisitiones arithmeticae* (1801) became a key text for many years to come: modular arithmetic, quadratic forms, cyclotomy, ...

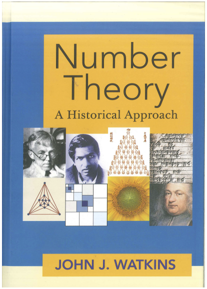
Number-theoretic problems (especially attempts to prove Fermat's Last Theorem) led to the development of ideal theory, and the linking of number theory and abstract algebra in algebraic number theory

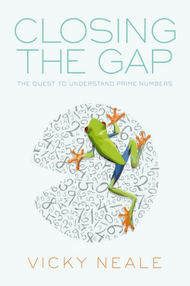
By the end of the 19th century, a new branch, analytic number theory, had also emerged (e.g., Riemann hypothesis, Prime Number Theory $\pi(x) \sim \frac{x}{\log x}, \ldots$)

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