



1763

# Supplementum quorundam theorematum arithmeticorum, quae in nonnullis demonstrationibus supponuntur

Leonhard Euler

Follow this and additional works at: <https://scholarlycommons.pacific.edu/euler-works>

 Part of the [Mathematics Commons](#)

Record Created:

2018-09-25

## Recommended Citation

Euler, Leonhard, "Supplementum quorundam theorematum arithmeticorum, quae in nonnullis demonstrationibus supponuntur" (1763). *Euler Archive - All Works*. 272.

<https://scholarlycommons.pacific.edu/euler-works/272>

## S V P P L E M E N T V M

### QVORVNDAM THEOREMATVM ARITHMETI- CORVM QVAE IN NONNVLLIS DEMONSTRATIONIBVS SVPPONVNTVR.

A u t o r e  
L. E V L E R O.

**C**um nuper demonstraviffem, non dari duos cubos, quorum summa fit cubus, sine sufficiente probatione assumferam, omnes numeros in hac forma contentos  $mm + mn + nn$ , quae forma facile ad hanc reducitur:  $pp + 3qq$ , nunquam alios admittere divifores, nisi qui ipsi in eadem forma contineatur. Atque hinc conclusi, si forma  $mm + mn + nn$  fuerit cubus, aliaue potestas, eius radicem quoque numerum eiusdem formae esse futuram; cui fundamento etiam tota demonstratio modo memorata innititur. Cum deinceps methodum novam et maxime generalem exposuiffem, tres cubos inveniendi, quorum summa fit cubus, quae simul omnibus adhuc vfitatis facilitate longe praestabat, non solum eandem indolem numerorum, in forma  $mm + mn + nn$ , seu  $pp + 3qq$ , contentorum, tanquam certam assumfi, sed etiam in evolutione solutionis supposui, huius generis numeros alios divifores primos, praeter ternarium, non implicare, nisi qui essent formae  $6x + 1$ . Quin etiam viciffim affirmare licet, omnes numeros primos istius formae  $6x + 1$ , cuiusmodi sunt 7, 13, 19, 31, 37, 43, etc. ita esse comparatos, vt in forma  $pp + 3qq$  contineantur: veluti

$$7 = 2^2 + 3 \cdot 1^2; 13 = 1^2 + 3 \cdot 2^2; 19 = 4^2 + 3 \cdot 1^2; 31 = 2^2 + 3 \cdot 3^2; \text{etc.}$$

Tom. VIII. Nou. Comm.

O

Quae

Quae Theoremata, etsi iam a Fermatio fuerant prolata, nusquam tamen adhuc demonstrata reperiuntur: ex quo operae pretium me facturum putavi, si has assertiones rigidis demonstrationibus confirmarem, quo simul supra memoratae demonstrationes ad summum certitudinis gradum eueherentur.

His proprietatibus innituntur ratiocinia, quibus summa deductus, ad tres cubos, quorum summa itidem est cubus, hinc autem omittis ratiociniis solutio consueto modo adornari poterit, idoneis formis pro radicibus cuborum assumendis. Quarum ratio etsi non perspiciatur, tamen in hoc Analyseos genere problemata plerumque per huiusmodi formulas feliciter excogitatas resolui solent, in quas saepe numero, vel casu, vel post plurima tentamina, incidimus.

Ita si tres cubi inueniri debeant, quorum summa sit cubus, positis eorum radicibus  $x$ ,  $y$ , et  $z$ , statuatur

$$x^3 + y^3 + z^3 = v^3.$$

Tum vero istorum cuborum radicibus sequentes formae tribuantur:

$$\begin{aligned} x &= (m-n)p + qq; & z &= pp - (m+n)q \\ y &= (m+n)p - qq; & v &= pp + (m-n)q \end{aligned}$$

et quoniam loco quaternarum quantitatum  $x$ ,  $y$ ,  $z$  et  $v$ , quaternae novae  $m$ ,  $n$ ,  $p$  et  $q$  in calculum introducuntur, his positionibus problema non restringi est censendum. Cum igitur vi problematis esse oporteat

$$x^3 + y^3 = v^3 - z^3, \text{ siue}$$

$$(x+y)(xx-xy+yy) = (v-z)(vv+vz+zz)$$

per assumtas formas habebitur:

 $x+y$

$x + y = 2mp$ ;  $xx - xy + yy = (mm + 3nn)pp - 6npqq + 3q^3$   
 $v - z = 2mq$ ;  $vv + vz + zz = 3p^3 - 6ppq + (mm + 3nn)qq$   
 hisque valoribus substitutis obtinebitur, diuisione vtrunque  
 per  $2m$  facta:

$$(mm + 3nn)p^3 - 6npqq + 3p^3q = 3p^3q - 6npqq + (mm + 3nn)q^3$$

vbi cum termini medii se vtrunque destruant, fiet

$$(mm + 3nn)(p^3 - q^3) = 3p^3q - 3p^3q = 3pq(p^3 - q^3)$$

Hic igitur commodo vsu venit, vt haec aequatio per  
 $p^3 - q^3$  diuidi queat, in quo ipso summa vtilitas nostrarum  
 positionum consistit; nanciscimur enim hanc aequationem

$$mm + 3nn = 3pq$$

vnde assumtis numeris  $m$  et  $n$  cum altero reliquorum  
 $p$  vel  $q$  pro lubitu alter sponte et quidem rationaliter  
 determinatur, quod eximium commodum non locum  
 haberet, nisi postrema aequatio diuisionem per  $p^3 - q^3$   
 admisisset. Nisi ergo fractiones euitare velimus, habebi-  
 mus statim

$$q = \frac{mm + 3nn}{3p}$$

Verum etsi fractiones facile erui possunt, dum aequae multi-  
 pla quaecunque radicem  $x$ ,  $y$ ,  $z$  et  $v$  pariter satisfaciunt,  
 tamen ad expressiones simpliciores pertingemus, si nu-  
 meros  $m$  et  $n$  statim ita assumamus, vt  $mm + 3nn$  pri-  
 mo diuisibile euadat per  $3$ , tum vero insuper duos  
 contineat factores, quorum alter pro  $p$ , alter pro  $q$  ac-  
 cipi queat.

Primo igitur statuatur  $m = 3k$ , vt fiat

$$pq = nn + 3kk$$

et quia, vt mox demonstrabo, numeri formae  $mm + 3kk$

alios non admittunt diuisores, nisi qui ipsi sint eiusdem formae, ponamus:

$$nn + 3kk = (aa + 3bb)(cc + 3dd)$$

vt fit:

$$p = aa + 3bb \text{ et } q = cc + 3dd$$

eritque

$$\text{vel } n = ac + 3bd; k = bc - ad; m = 3bc - 3ad$$

$$\text{vel } n = ac - 3bd; k = bc + ad; m = 3bc + 3ad$$

Hanc pluralitatem valorum per ambiguitatem signorum ita exhibere poterimus, vt fit

$$m = \pm 3(bc \pm ad): n = \pm (ac \mp 3bd)$$

ideoque diuersi valores pro  $m$  et  $n$ , sumtis pro  $a, b, c, d$ , numeris quibuscunque, erunt

$$\text{I. } m + n = 3(bc + ad) + (ac - 3bd); m - n = 3(bc + ad) - (ac - 3bd)$$

$$\text{II. } m + n = 3(bc + ad) - (ac + 3bd); m - n = 3(bc + ad) + (ac - 3bd)$$

$$\text{III. } m + n = 3(bc - ad) + (ac + 3bd); m - n = 3(bc - ad) - (ac + 3bd)$$

$$\text{IV. } m + n = 3(bc - ad) - (ac + 3bd); m - n = 3(bc - ad) + (ac + 3bd)$$

Hinc autem sequuntur solutiones, quas iam dudum fuis exposui, quare ad propositum reuertor, sequentes propositiones demonstraturus.

### Propositio I.

1. Si numeri  $a$  et  $b$  non sint numeri inter se primi, tum numerus  $aa + 3bb$  non erit primus, sed diuisibilis erit per quadratum maximi communis diuisoris numerorum  $a$  et  $b$ .

Demon-

## Demonstratio.

Sit enim  $m$  maximus communis diuisor numero-  
rum  $a$  et  $b$ , ita vt fit  $a=mc$  et  $b=md$ , existentibus  
iam  $c$  et  $d$  numeris inter se primis, quia alioquin non  
esset maximus communis diuisor. Ac numerus  $aa+3bb$   
induet hanc formam:  $mm(cc+3dd)$ , quae propterea  
certo diuisorem habet  $mm$ .

## Coroll. 1.

2. Nisi ergo numeri  $a$  et  $b$  sint primi inter se,  
numerus ex iis formatus  $aa+3bb$  primus esse nequit.  
Neque vero hinc vicissim concludere licet, numerum  
 $aa+3bb$  semper esse primum, quoties numeri  $a$  et  $b$   
fuerint primi inter se.

## Coroll. 2.

3. Primo autem patet, numerum  $aa+3bb$  di-  
uisibilem esse per ternarium, dum numerus  $a$  fuerit  
multipulum ternarii, etiamsi caeterum  $a$  et  $b$  fuerint  
numeri primi inter se. Neque vero vnquam forma  
 $aa+3bb$  per 9 altiore vel ternarii potestatem est  
diuisibilis, nisi ambo numeri  $a$  et  $b$  communem diui-  
forem habeant 3.

## Coroll. 3.

4. Deinde etiam patet, formam  $aa+3bb$  nu-  
merum parem esse non posse, nisi ambo numeri  $a$   
et  $b$  vel sint pares, vel impares. Vtroque autem casu  
numerus  $aa+3bb$  non solum per 2, sed etiam per  
4 erit diuisibilis.

## Coroll. 4.

5. Non ergo datur numerus formae  $aa+3bb$ , qui sit impariter par, sed statim atque admittit diuisorem 2, simul erit diuisibilis per 4. Unde quoties huiusmodi numeri fuerint pares, quaternarium, tanquam eorum factorem simplicem, considerare licet, etiamsi alias quaternarius, utpote binarii quadratum, non inter numeros primos referatur.

## Coroll. 5.

6. Si ergo numerus formae  $aa+3bb$  sit primus, non solum certo constat, ambos numeros  $a$  et  $b$  esse primos inter se, sed etiam utrumque non esse impar. Necessè igitur est, ut alter sit par, alter vero impar.

## Propositio II.

7. Si numerus formae  $aa+3bb$  per ternarium est diuisibilis, tunc etiam quotus est numerus formae eiusdem.

## Demonstratio.

Si numerus  $aa+3bb$  per 3 est diuisibilis, necesse est, ut radix prioris quadrati  $a$  sit multipulum ternarii. Ponamus ergo  $a=3c$ , et numerus propositus erit  $9cc+3bb$ , qui per 3 diuisus dat quotum  $3cc+bb$ , qui utique est numerus eiusdem formae  $aa+3bb$ .

## Scholion.

8. Notari hic conuenit ipsum quoque ternarium esse numerum formae  $aa+3bb$ , quippe qui prodit, si  $a=0$  et  $b=1$ . Consideramus autem has duas formas  $aa+3bb$  et  $mm+mn+nn$  tanquam aequivalentes, quoniam

quoniam posterior in priorem transit, ponendo  $m = a + b$ ,  
 et  $n = b - a$ ; unde quicquid de altera demonstramus,  
 etiam de altera valet. Posterior autem, casu  $m = 1$   
 et  $n = 1$ , manifesto dat 3. Videtur quidem forma  
 $mm + mn + nn$ , si numerorum  $m$  et  $n$  alter fuerit par,  
 alter impar, ad priorem reduci non posse, quia tum  
 in integris esse nequit  $m = a + b$ , et  $n = b - a$ ; verum  
 dantur adhuc aliae reductiones, scilicet  $a = \frac{1}{2}m + n$ , et  
 $b = m$ , siue  $a = m + \frac{1}{2}n$ , et  $b = n$ , quarum ope, si nu-  
 merorum  $m$  et  $n$  alter fuerit par, alter impar, forma  
 $mm + mn + nn$  ad  $aa + 3bb$  reducitur.

### Propositio III.

9. Si numerus formae  $aa + 3bb$  per quaterna-  
 rium est diuisibilis, tum etiam quotus erit numerus eius-  
 dem formae  $aa + 3bb$ .

### Demonstratio.

Diuisio formae  $aa + 3bb$  per 4 succedit, si  
 vel vterque numerorum  $a$  et  $b$  fuerit par, vel impar.  
 Priori casu ponatur  $a = 2c$ , et  $b = 2d$ , fietque  $aa + 3bb$   
 $= 4cc + 12dd$ , unde, diuisione per 4 instituta, prodit  
 quotus  $cc + 3dd$ .

Sin autem vterque numerus  $a$  et  $b$  fuerit impar,  
 tum eorum, vel summa, vel differentia, certo erit diui-  
 sibilis per 4. Namque, cum tam  $a + b$ , quam  $a - b$ , sit  
 numerus par, eorumque summa sit  $2a$ , hoc est nume-  
 rus impariter par, necesse est, vt alter eorum sit im-  
 pariter par, alter vero pariter par. Erit ergo, vel

$a + b$



$a + b = 4c$ , vel  $a - b = 4c$ , ideoque  $a = 4c \pm b$ : quo valore substituto fiet

$$aa + 3bb = 16cc \pm 8bc + 4bb$$

unde, diuisione per 4 instituta, prodit quotus

$$4cc \pm 2bc + bb = (b \pm c)^2 + 3cc.$$

### Coroll. 1.

10. Hic pariter notasse iuuabit, ipsum quaternarium etiam esse numerum formae  $aa + 3bb$ , inde resultantem, positis  $a = 1$ , et  $b = 1$ . At ex forma  $mm + mn + nn$  quaternarius nascitur, si ponatur  $n = 0$ , et  $m = 2$ .

### Coroll. 2.

11. Cum igitur viderimus, dari numeros formae  $aa + 3bb$ , qui iam per 3, quam per 4, sint diuisibiles: nunc demonstrauimus, quotos ex vtraque diuisione resultantes etiam esse numeros eiusdem formae  $aa + 3bb$ .

### Coroll. 3.

12. Quodsi autem ambo numeri  $a$  et  $b$  fuerint impares, tum quotus, ex diuisione numeri  $aa + 3bb$  per 4 nascens, erit numerus impar. Vidimus enim, quotum esse  $4cc \pm 2bc + bb$ , qui, ob  $b$  numerum imparem, certo est impar.

### Scholion.

13. Quod hactenus de diuisione numerorum formae  $aa + 3bb$  per 3 et 4 demonstrauimus, idem demonstrabimus de diuisione per numerum quemcumque alium

aliud primum formae  $aa + 3bb$ ; quotum scilicet inde oriundum pariter fore numerum eiusdem formae. Hunc in finem, ut breuitati consulamus, denotabunt litterae P, Q, R, S etc. numeros primos formae  $aa + 3bb$ , inter quos tamen etiam quaternarium referemus, etiamsi non sit primus, propterea quod binarius ab hac forma est excludendus.

### Propositio IV.

14. Si numerus formae  $aa + 3bb$  est diuisibilis per numerum primum  $P = pp + 3qq$ , tum quotus est etiam numerus eiusdem formae.

### Demonstratio.

Si  $aa + 3bb$  est diuisibilis per  $pp + 3qq$ , tum etiam  $aapp + 3bbpp$  per eundem est diuisibilis, itemque  $aapp + 3aaqq$ ; quare etiam horum numerorum differentia  $3aaqq - 3bbpp$ , ideoque et  $aaqq - bbpp = (aq + bp)(aq - bp)$ . Cum igitur  $3pp + 3qq$  sit numerus primus, necesse est, ut alteruter istorum factorum, scilicet vel  $aq + bp$ , vel  $aq - bp$ , sit per  $pp + 3qq$  diuisibilis. Ponatur ergo pro utroque casu  $aq + bp = m(pp + 3qq)$ ; hincque fiet

$$a = \frac{m(pp + 3qq)}{q} + \frac{bp}{q} = 3mq + \frac{p}{q}(mp + b).$$

Verum quia  $a$  est numerus integer, et  $p$  et  $q$  numeri inter se primi, necesse est, ut  $mp + b$  diuisionem per  $q$  admittat. Ponatur ergo  $mp + b = nq$ , eritque

$$b = mp + nq \quad \text{et} \quad a = 3mq + np$$

Cum igitur numeri  $a$  et  $b$  necessario hoc modo expri-

mantur, siquidem numerus  $aa + 3bb$  per  $pp + 3qq$  fuerit diuisibilis, hinc obtinebimus

$$aa + 3bb = 3mmp + 9mmq + 3nnq + nnp \\ = (pp + 3qq)(nn + 3mm)$$

vnde patet, hunc numerum, per numerum primum  $P = pp + 3qq$  diuisum, pro quoto dare  $nn + 3mm$ , hoc est numerum formae  $aa + 3bb$ .

### Coroll. 1.

15. Quoties ergo numerus formae  $aa + 3bb$  diuisorem primum habet  $P = pp + 3qq$ , quotus est numerus formae  $nn + 3mm$ . Vel, quod eodem redit, si numerus  $aa + 3bb$  constet duobus factoribus, quorum alter sit primus  $P = pp + 3qq$ , tum etiam alter factor siue sit numerus primus, siue compositus, erit numerus formae  $nn + 3mm$ .

### Coroll. 2.

16. Si igitur numerus  $aa + 3bb$  duobus constaret factoribus, quorum alter non in forma  $nn + 3mm$  contineretur, tum alter certe non erit primus formae  $pp + 3qq$ .

### Coroll. 3.

17. Ex demonstratione patet, quomodo innumerabiles numeri  $aa + 3bb$  exhiberi queant, qui omnes sint diuisibiles per  $pp + 3qq$ ; eiusmodi nempe numeri obtinentur capiendo

$$a = 3mq + np \quad \text{et} \quad b = mp + nq$$

neque

neque hic amplius opus est, conditionem adiecisse, ut  $pp+3qq$  sit numerus primus; quoniam his valoribus assumtis in genere fit  $aa+3bb=(pp+3qq)(nn+3mm)$ .

### Coroll. 4.

18. Hinc igitur vicissim intelligitur, si duo pluresue numeri quicunque formae  $aa+3bb$  in se inuicem multiplicentur, productum semper fore numerum eiusdem formae. Quod enim de producto duorum valet, facile ad productum quocunque talium numerorum extenditur.

### Scholion.

19. Etiam si autem verum sit, productum ex duobus numeris formae  $aa+3bb$  itidem esse numerum eiusdem formae, tamen hinc per legitimam consequentiam nondum inferre licet, si numerus formae  $aa+3bb$  diuisorem habeat quemcunque  $pp+3qq$ , tum etiam quotum eiusdem formae esse futurum: tamen si enim et hoc verum sit, tamen peculiari indiget demonstratione mox exponenda. Eiusmodi autem conclusionem illicitam esse, vel ex hoc exemplo patebit: cum productum ex duobus numeris paribus sit numerus par, si quis inde concludere vellet, numerum parem per parem diuisum quotum etiam parem esse praebiturum, is certe falleretur. Demonstrationem ergo huius veritatis a diuisore primo formae  $pp+3qq$  sum exorsus, quae conditio eatenus demonstrationem afficit, quod absque ea perperam concluderetur, cum pro-

ductum  $(aq + bp)(aq - bp)$  sit diuisibile, alterutrum factorem diuisibilem esse debere per  $pp + 3qq$ . Deinde vero etiam ex eo, quod  $p$  et  $q$  sint numeri inter se primi, deriuauimus producti  $p(mp + b)$ , quod per  $q$  est diuisibile, factorem  $mp + b$  per  $q$  diuisibilem esse debere; quae posterior conditio cum priora necessario est connexa.

### Propositio V.

20. Si numerus  $aa + 3bb$  fuerit diuisibilis per productum ex duobus pluribusue numeris primis formae  $pp + 3qq$ , tum etiam quotus erit numerus eiusdem formae, puta  $nn + 3mm$ .

### Demonstratio.

Sint enim  $P, Q, R$ , etc. numeri primi formae  $pp + 3qq$ , numerusque  $aa + 3bb$  diuisibilis per productum  $PQR$ . Sit  $M$  quotus inde resultans, ita ut sit  $aa + 3bb = MPQR$ . Cum igitur sit  $\frac{aa + 3bb}{P} = MQR$ , erit per prop. praec.  $MQR$  numerus eiusdem formae. Ponatur itaque  $MQR = cc + 3dd$ , erit  $\frac{cc + 3dd}{Q} = MR$ ; ideoque, ob eandem rationem, hic quotus  $MR$  numerus eiusdem formae statuatur, itaque  $MR = ee + 3ff$ , et cum sit  $\frac{ee + 3ff}{R} = M$ , erit pariter  $M$  numerus formae  $nn + 3mm$ .

### Coroll. I.

21. Si ergo numerus  $aa + 3bb$  fuerit productum ex numeris quocunque primis  $P, Q, R, S$  etc. formae

formae  $pp + 3qq$ , et praeterea numero  $M$ , ita ut fit  $aa + 3bb = MPQRS$ , certo affirmare poterimus, hunc numerum  $M$  esse eiusdem formae seu  $M = nn + 3mm$ .

Coroll. 2.

22. Quodsi igitur numerus  $aa + 3bb$  vnum habeat factorem  $A$ , qui non sit numerus formae  $nn + 3mm$ , tum alter factor neque erit numerus primus formae  $pp + 3qq$ , neque productum ex duobus pluribusue huiusmodi numeris primis.

Coroll. 3.

23. Eodem ergo casu si ponamus  $aa + 3bb = AB$ , et  $A$  non fuerit numerus formae  $nn + 3mm$ ; tum  $B$  vnum saltem factorem primum complectetur, qui non erit huius formae. Nam si  $B$  est numerus primus, non erit formae  $pp + 3qq$ , sin autem non est primus, quia non ex meris numeris primis formae  $pp + 3qq$  constabit, vnum ad minimum factorem continebit, qui non sit eiusdem formae.

Coroll. 4.

24. At si existente  $aa + 3bb = AB$ , factor  $A$  non fuerit numerus formae  $nn + 3mm$ , tum vel ipse erit numerus primus, in hac forma non contentus, vel saltem factorem implicabit primum, in hac forma non contentum; si enim  $A$  ex meris numeris primis formae  $pp + 3qq$  esset conflatus, ipse foret numerus eiusdem formae.

## Coroll. 5.

25. Hinc sequitur, si numerus  $aa+3bb$  vnum habeat factorem primum in forma  $pp+3qq$  non contentum, tum eum insuper certo adhuc alium factorem inuoluere, qui aequae non in hac forma  $pp+3qq$  contineatur.

## Coroll. 6.

26. Ita iam ante vidimus, si numerus  $aa+3bb$  sit par, seu factorem habeat 2, qui numerus non est formae  $pp+3qq$ , tum eum insuper eundem factorem 2 complecti, seu non solum per 2, sed etiam per 4, esse diuisibilem.

## Scholion.

27. Exhiberi quidem possunt numeri formae  $aa+3bb$ , qui per numerum quemcunque  $N$  sint diuisibiles, etiam si  $N$  non sit numerus formae  $pp+3qq$ ; dum scilicet pro  $a$  et  $b$  multipla quaecunque huius numeri  $N$  accipiuntur: ita posito  $a=mn$ , et  $b=nn$ , numerus  $aa+3bb=NN(mm+3nn)$ , non solum per  $N$ , sed adeo per eius quadratum  $NN$ , sit diuisibilis; hocque ergo casu utique duo adsunt factores  $N$  et  $N$ , quorum neuter in forma  $pp+3qq$  continetur, uti §. 25. ostendimus. Verum si  $a$  et  $b$  sint numeri inter se primi, hic casus locum habere nequit, ex quo merito dubitamus, num numerus inde formatus  $aa+3bb$  praeter binarium vllam admittat diuisorem, qui non sit formae  $pp+3qq$ ? De binario quidem hoc negari nequit, cum quoties  $a$  et  $b$  fuerint numeri impares ambo, diuisio per 2 succedat, at vero tum insuper binarius

rius inest, qui cum illo coniunctus præbet factorem 4, quasi simplicem spectandum. Diligentius igitur examinandum restat, utrum, dum  $a$  et  $b$  sunt primi inter se, numerus  $aa+3bb$  habeat vllum divisorem primum, qui non in forma  $pp+3qq$  contineatur, nec ne? quod quidem esse negandum mox rigide sum demonstraturus; in quo negotio autem probe est cauendum, ne casus binarii, quem excipi oportet, in demonstratione quicquam turbet.

### Propositio VI.

28. Si daretur numerus primus  $A$ , in forma  $pp+3qq$  non contentus, qui esset divisor cuiuspiam numeri  $aa+3bb$ , numeris  $a$  et  $b$  existentibus inter se primis, tum exhiberi posset alius numerus primus præter binarium, minor  $B$ , in forma  $pp+3qq$  pariter non contentus, qui etiam futurus esset divisor cuiuspiam numeri formæ  $aa+3bb$ , in quo numeri  $a$  et  $b$  itidem forent inter se primi.

### Demonstratio.

Quia  $a$  et  $b$  sunt numeri primi inter se, et  $aa+3bb$  per  $A$  divisibilis ponitur, erunt ii quoque primi ad  $A$ . Si illi numeri essent maiores, quam  $A$ , statui posset  $a=mA+c$ , et  $b=nA+d$ , ut numeri  $c$  et  $d$ , qui pariter tum inter se, quam ad  $A$ , futuri essent primi, forent semissi ipsius  $A$  minores, scilicet  $c < \frac{1}{2}A$  et  $d < \frac{1}{2}A$ , quia  $A$ , ut pote primus, est impar, casum enim quo  $A=2$  hinc excipimus. Proderet autem hac positione

$$aa+3bb = mmAA + 2mAc + cc + 3nnAA + 6nd + 3dd$$

hincque



hincque obtineretur numerus  $cc + 3dd$  minor, quam  $AA$ , qui esset per  $A$  diuisibilis, et quotus foret minor, quam  $A$ . Cum igitur  $A$  sit per hypothesein numerus in forma  $pp + 3qq$  non contentus, vel ipse quotus, si fuerit primus, non erit numerus formae  $pp + 3qq$ , vel, si sit compositus, factorem habebit primum in hac forma non contentum. Sit  $B$  vel ipse quotus vel iste eius factor, eritque certe  $B < A$ , ex quo daretur numerus primus  $B$  minor, quam  $A$ , in forma  $pp + 3qq$  non contentus, qui esset diuisor numeri  $cc + 3dd$ , existentibus numeris  $c$  et  $d$  inter se primis.

Dico autem hunc numerum primum  $B$  a binario fore diuersum. Vel enim quotus  $\frac{cc + 3dd}{A}$  foret impar, vel par: et casu priori binarius in eo non contineretur, sicque numerus  $B$  non esset 2. Casu autem posteriori quotus binarium quidem, atque adeo quaternarium involueret; vnde cum 4 sit numerus formae  $pp + 3qq$ , necesse esset, vt ille quotus alium insuper factorem primum in forma  $pp + 3qq$  non contentum implicaret. Vel si  $cc + 3dd$  esset per 4 diuisibilis, quod eueniret, si vterque numerus  $c$  et  $d$  esset impar, eius quadrans  $\frac{1}{4}(cc + 3dd)$  ad formam  $ee + 3ff$  reduci possit, quae cum per  $A$  etiam nunc foret diuisibilis, multo magis quotus  $\frac{ee + 3ff}{A}$  implicaret factorem primum imparem in forma  $pp + 3qq$  non contentum.

### Propositio VII.

29. Omnes numeri huius formae  $aa + 3bb$ , siquidem  $a$  et  $b$  sint numeri primi inter se, praeter binarium nullos admittunt diuisores primos, nisi qui ipsi in forma  $pp + 3qq$  contineantur. Demon-

## Demonstratio.

Si enim numerus quispiam formae  $aa + 3bb$  haberet factorem primum quantumvis magnum  $A$ , qui in forma  $pp + 3qq$  non contineretur, ex eo inueniri posset alius numerus primus  $B$ , minor quam  $A$ , nec in forma  $pp + 3qq$  contentus, qui pariter esset diuisor cuiuspiam numeri formae  $aa + 3bb$ , existentibus  $a$  et  $b$  numeris inter se primis; atque ex hoc numero  $B$  simili modo alii  $C$ ,  $D$ ,  $E$  continuo minores eiusdem indolis inueniri possent, haecque diminutio nunquam terminaretur, neque etiam vnquam ad binarium perueniretur. Cum igitur exhibitio numerorum integrorum continuo minorum inuoluat contradictionem: sequitur, praeter binarium nullum dari numerum primum in forma  $pp + 3qq$  non contentum, per quem vllus numerus formae  $aa + 3bb$  diuidi queat, existentibus  $a$  et  $b$  numeris inter se primis.

## Coroll. 1.

30. Omnes ergo diuisores primi, qui conueniunt numeris formae  $aa + 3bb$ , siquidem  $a$  et  $b$  sint numeri inter se primi, ipsi in eadem forma  $pp + 3qq$  continentur; dummodo hinc binarius excludatur.

## Coroll. 2.

31. Si igitur numeri primi in duas classes distribuuntur, quarum prior contineat eos, qui sunt formae  $pp + 3qq$ ; posterior vero eos, qui ad hanc formam  
 Tom. VIII. Nou. Comm. Q reduci

reduci nequeunt : omnes numeri huius posterioris classis ex serie diuisorum numerorum formae  $aa + 3bb$  excluduntur.

### Coroll. 3.

32. Nisi ergo numerus  $aa + 3bb$ , existentibus  $a$  et  $b$  numeris inter se primis, ipse sit primus, erit is productum ex meris numeris primis formae  $pp + 3qq$ ; dummodo quaternarius etiam inter hos numeros referatur.

### Scholion.

33. Quod productum ex duobus pluribusque numeris formae  $pp + 3qq$  iterum in forma  $aa + 3bb$  contineatur, supra ostendimus; indeque ergo patebat, si  $P$ ,  $Q$ ,  $R$ ,  $S$ , etc. denotent numeros primos in forma  $pp + 3qq$  contentos, productum ex quocunque huiusmodi numeris  $P$ ,  $Q$ ,  $R$ ,  $S$ , etc. semper ad formam  $aa + 3bb$  reuocari posse. Nunc autem huius propositionis inuersam demonstrauimus, qua patet, numeros formae  $aa + 3bb$  nullos alios factores admittere, nisi qui ipsi sint numeri formae  $pp + 3qq$ . Hic quidem assumimus, numeros  $a$  et  $b$  esse primos inter se: si autem non essent primi, sed maximum haberent diuisorem communem  $m$ , ut sit  $a = mc$ , et  $b = md$ , tum numerus  $aa + 3bb = mm(cc + 3dd)$  primum habebit factorem quadratum  $mm$ , cuius radix potest esse numerus quicunque, praeterea vero alios non in-

uoluet

voluet factores primos, nisi qui ipsi sint formae  $pp+3qq$ .

### Propositio VIII.

34. Omnis numerus primus formae  $pp+3qq$ , si per 6 diuidatur, relinquit unitatem, seu in forma numerorum  $6n+1$  continetur; excepto ternario, qui etiam in forma  $pp+3qq$  continetur.

### Demonstratio.

Cum  $pp+3qq$  sit numerus primus, quadratum  $pp$  per ternarium non est diuisibile, sed per 3 diuisum relinquit 1; quia ergo  $3qq$  diuisionem per 3 admittit, summa  $pp+3qq$  per 3 diuisa residuum dabit  $=1$ ; eritque propterea numerus formae  $3m+1$ . Cum autem  $pp+3qq$  simul sit numerus impar per hypothesin, necesse est, vt  $m$  sit numerus par; vnde, posito  $m=2n$ , formula  $6n+1$  omnes complectetur numeros primos in forma  $pp+3qq$  contentos; excepto scilicet ternario ipso, cuius singularis est ratio.

### Coroll. 1.

35. Quia omnes numeri primi, exceptis 2 et 3, vel in hac formula  $6n+1$ , vel in hac  $6n-2$ , continentur, euidentis est, nullos numeros primos posterioris formae  $6n-1$ , in forma  $pp+3qq$  contineri.

Q 2

Coroll.

## Coroll. 2.

36. Hinc omnes numeri primi formae  $6n-1$  qui sunt :

5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89, etc. ex diuisoribus numerorum formae  $aa+3bb$  sunt excludendi, seu nullus numerus huius formae  $aa+3bb$ , dum quidem sint  $a$  et  $b$  numeri primi inter se, exhiberi potest, qui per vllum numerum primum formae  $6n-1$  fit diuisibilis.

## Scholion.

37. Vtrum autem omnes numeri primi alterius formae  $6n+1$ , qui sunt :

7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, etc. sint diuisores numerorum formae  $aa+3bb$ ; seu, quod eodem redit, an omnes in forma  $pp+3qq$  contineantur? ex allatis nondum affirmare licet. Inde enim tantum constat, omnes numeros primos formae  $pp+3qq$  simul in forma  $6n+1$  contineri, et propositio inuersa peculiari indiget demonstratione; quae ita concinnari debet, vt, proposito numero primo formae  $6n+1$  quocunque, ostendatur, semper quempiam numerum formae  $aa+3bb$ , in quo  $a$  et  $b$  sint numeri primi inter se, exhiberi posse, qui per illum numerum  $6n+1$  fit diuisibilis: in quo negotio loco formae  $aa+3bb$  etiam haec  $ff+fg+gg$  illi aequiualens accipi potest. Si enim numerum  $f$  et  $g$  alteruter, puta  $g$ , fuerit par, erit

$$ff+fg+gg=(f\pm\frac{1}{2}g)^2+3(\frac{1}{2}g)^2$$

fin

sin autem vterque sit impar, erit tam  $f+g$ , quam  $f-g$ , numerus par, et

$$ff + fg + gg = \frac{(f+g)^2}{2} + 3 \frac{(f-g)^2}{2}.$$

Quodsi ergo exhiberi queat numerus  $ff + fg + gg$  per numerum primum  $6n+1$  diuisibilis, ita vt  $f$  et  $g$  sint primi inter se, simul constabit, numerum  $6n+1$  esse numerum in forma  $pp + 3qq$  contentum; id quod in sequente propositione demonstrabimus.

### Propositio IX.

38. Omnis numerus primus formae  $6n+1$  simul in hac forma  $pp + 3qq$  continetur.

### Demonstratio.

Iam dudum demonstraui, si  $6n+1$  fuerit numerus primus, per eum diuisibiles esse omnes numeros in hac forma  $a^{6n} - b^{6n}$  contentos, dummodo neuter numerorum  $a$  et  $b$  seorsim per  $6n+1$  sit diuisibilis. Cum igitur in factores resoluendo sit

$$a^{6n} - b^{6n} = (a^{2n} - b^{2n})(a^{4n} + a^{2n}b^{2n} + b^{4n})$$

alteruter horum factorum per  $6n+1$  sit diuisibilis necesse est. Quodsi ergo dentur casus, quibus factor  $a^{2n} - b^{2n}$  non sit diuisibilis per  $6n+1$ , vt tamen, neque  $a$ , neque  $b$ , per eum sit diuisibilis, iis casibus certe alter factor  $a^{4n} + a^{2n}b^{2n} + b^{4n}$ , hoc est numerus formae  $ff + fg + gg$ , per  $6n+1$  erit diuisibilis, ideoque numerus primus  $6n+1$  foret in forma  $pp + 3qq$  contentus. Demonstrari igitur debet, dari casus, quibus

Q 3

forma

forma  $a^{2n} - b^{2n}$  non sit diuisibilis per  $6n + 1$ . Ad hoc efficiendum sumo  $b = 1$ , et ostendam, fieri non posse, vt omnes isti numeri:

$$2^{2n} - 1; 3^{2n} - 1; 4^{2n} - 1; 5^{2n} - 1; \dots (6n)^{2n} - 1;$$

sint per  $6n + 1$  diuisibiles, vbi quidem pro  $a$  omnes numeros ipso  $6n + 1$  minores, ideoque primos ad eum, assumi pono. Nam si omnes hi numeri per  $6n + 1$  essent diuisibiles, eorum etiam differentiae, cum primae, tum secundae, et sequentes omnes, per  $6n + 1$  essent diuisibiles, ideoque etiam differentiae ordinis  $2n$ , quae sunt omnes constantes, et hoc modo exprimentur:

$$2^{2n} - \frac{2^n}{1} \cdot 3^{2n} + \frac{2^n(2n-1)}{1 \cdot 2} 4^{2n} - \frac{2^n(2n-1)(2n-2)}{1 \cdot 2 \cdot 3} 5^{2n} \dots (2+2n)^{2n}$$

vbi, cum sit  $2n + 2 < 6n$ , nullae potestates numerorum per  $6n + 1$  diuisibilium ingrediuntur. Aliunde autem constat, differentiam ordinis  $2n$  esse  $= 1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot 2n$ , quae, cum certe non sit per  $6n + 1$  diuisibilis, manifesto indicat, reperiri adeo inter hos numeros:

$$2^{2n} - 1; 3^{2n} - 1; 4^{2n} - 1; \dots (2 + 2n)^{2n} - 1$$

vnum, vel etiam plures, qui non sint per  $6n + 1$  diuisibiles. Dum autem vnicus detur huiusmodi numerus  $a^{2n} - 1$  per  $6n + 1$  non diuisibilis, per eum erit diuisibilis  $a^{4n} + a^{2n} + 1$ , hoc est numerus formae  $ff + fg + gg$ , in quo neque  $f$ , neque  $g$ , sit per  $6n + 1$  diuisibilis. Consequenter numerus primus  $6n + 1$  est formae  $pp + 3qq$ .

### Scholion.

39. Omnia ergo, quae cum in demonstratione Theorematis, non dari duos cubos, quorum summa sit cubus,

cubus, tum in solutione problematis de inveniendis tribus cubis, quorum summa sit cubus, assumseram, iam plane rigide sunt demonstrata. Assumseram autem primo, numeros formae  $aa + 3bb$ , seu  $ff + fg + gg$ , nullos admittere diuisores primos, nisi qui ipsi sint eiusdem formae, deinde omnes numeros primos istius formae simul in formula  $6n + 1$  contineri, ac vicissim omnes numeros primos in formula  $6n + 1$  contentos, simul esse numeros formae  $pp + 3qq$ . Quare nunc, tam illa demonstratio, quam solutio, pro perfectis sunt habendae. Interim tamen fateri cogor, in hac de natura numerorum Theoria plurima etiamnum desiderari, atque *Fermatii* demonstrationes deperditas sine dubio multo profundiores speculationes in se esse complexas. Eo enim modo, quo usus sum ad demonstrandum, summam duorum cuborum nunquam posse esse cubum, non perspicio, quomodo demonstratio ad potestates altiores extendi possit; cum tamen *Fermatius* demonstrationem habuerit, neque summam  $a^n + b^n$ , neque differentiam  $a^n - b^n$ , nunquam esse potestatem similis exponentis  $c^n$ , quando exponens  $n$  fuerit binario maior. Demonstrandum ergo esset, hanc aequationem  $a^n + b^n = c^n$  in rationalibus nunquam locum habere posse, statim atque exponens  $n$  binarium superet, nisi vnus numerorum  $a, b, c$  euanescat. Deinde etsi demonstrauit, numeros primos omnes formae  $6n + 1$  esse in formula  $pp + 3qq$  contentos, tamen simili modo demonstrare non licet, numeros primos formae  $8n + 3$  semper in forma  $pp + 2qq$  contineri, quod tamen aequae est certum, et a *Fermatio* demonstratum.



## 128 THEOREMATA ARITHMETICA.

stratum. Successit mihi quidem demonstratio, quod numeri primi formae  $4n + 1$  sint omnes duorum quadratorum summae, similique modo demonstrare possum, omnes numeros primos formae  $8n + 1$  simul in forma  $pp + 2qq$  contineri: verum plurima eiusdem generis theoremata proferri possunt aequae vera, veluti quod omnes numeri primi vel huius formae  $20n + 1$ , vel  $20n + 9$ , simul in formula  $pp + 5qq$  contineantur, et huiusmodi plura alia, quae tamen nondum video, quomodo demonstrari queant. Ex quo Theoria numerorum nobis adhuc maximam partem abscondita est censenda.

---



---



---

CON.