1763

Supplementum quorundam theorematum arithmeticorum, quae in nonnullis demonstrationibus supponuntur

Leonhard Euler

SVPPLEMENTVM
QVORVNDAM THEOREMATVM ARITHMETICORVM QVAE IN NONNVLLIS DEMONSTRATIONIBVS SVPPONVNTVR.

Auctore
L. EVLERO.

Cum nuper demonstrauissem, non dari duos cubos, quorum summa sit cubus, sine sufficiente probatione assumseram, omnes numeros in hac forma contentos $mm+mn+nn$, quae forma facile ad hanc reducitur: $pp+3qq$, nunquam alios admittere diuisores, 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 nouam et maxime generalem exposuissem, tres cubos inueniendi, quorum summa sit cubus, quae simul omnibus adhuc vsitatis facilitate longe praestabat, non solum eandem indolem numerorum, in forma $mm+mn+nn$, seu $pp+3qq$, contentorum, tanquam certam assumsi, sed etiam in euolutione solutionis supposui, huius generis numeros alios diuisores primos, praeter ternarium, non implicare, nisi qui essent formae $6x+1$. Quin etiam vicissim 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

$7=2^2+3.1^2$; $13=1^2+3.2^2$; $19=4^2+3.1^2$; $31=2^2+3.3^2$; etc.

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

His proprietatibus innituntur ratiocinia, quibus sum deductus, ad tres cubos, quorum summa itidem est cubus, hinc autem omissis 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:

$$x = (m-n)p + qq; \qquad z = pp - (m+n)q$$
$$y = (m+n)p - qq; \qquad v = pp + (m-n)q$$

et quoniam loco quaternarum quantitatum x, y, z et v, quaternae nouae 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:

$x+y$

$x+y=2mp; xx-xy+yy=(mm+3nn)pp-6npqq+3q^4$
$v-z=2mq; vv+vz+zz=3p^4-6nppq+(mm+3nn)qq$
hisque valoribus substitutis obtinebitur, diuisione vtrinque per $2m$ facta:

$$(mm+3nn)p^3-6nppqq+3pq^4=3p^4q-6nppqq+(mm+3nn)q^3$$

vbi cum termini medii se vtrinque destruant, fiet

$$(mm+3nn)(p^3-q^3)=3p^4q-3pq^4=3pq(p^3-q^3)$$

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, habebimus statim

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

Verum etsi fractiones facile erui possunt, dum aeque multipla quaecunque radicum x, y, z et v pariter satisfaciunt, tamen ad expressiones simpliciores pertingemus, si numeros m et n statim ita assumamus, vt $mm+3nn$ primo diuisibile euadat per 3, tum vero insuper duos contineat factores, quorum alter pro p, alter pro q accipi queat.

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

$$pq=nn+3kk$$

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

 alios

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

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

vt sit:

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

eritque

vel $n = ac + 3bd$; $k = bc - ad$; $m = 3bc - 3ad$

vel $n = ac - 3bd$; $k = bc + ad$; $m = 3bc + 3ad$

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

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

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

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

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

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

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

Hinc autem sequuntur solutiones, quas iam dudum fusius 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 numerorum a et b, ita vt ſit $a = mc$ 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 $aa + 3bb$ diviſibilem eſſe per ternarium, dum numerus a fuerit multiplum ternarii, etiamſi caeterum a et b fuerint numeri primi inter ſe. Neque vero vnquam forma $aa + 3bb$ per 9 altiorem ve ternarii poteſtatem eſt diuiſibilis, niſi ambo numeri a et b communem diuiſorem habeant 3.

Coroll. 3.

4. Deinde etiam patet, formam $aa + 3bb$ numerum 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. Vnde quoties huiusmodi numeri fuerint pares, quaternarium, tanquam eorum factorem ſimplicem, conſiderare licet, etiamſi alias quaternarius, vtpote 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 vtrumque non eſſe imparem. Neceſſe igitur eſt, vt 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, vt radix prioris quadrati a ſit multiplum ternarii. Ponamus ergo $a=3c$, et numerus propoſitus erit $9cc+3bb$, qui per 3 diuiſus dat quotum $3cc+bb$, qui vtique 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 aequiualentes, quoniam

quoniam posterior in priorem transit, ponendo $m=a+b$, et $n=b-a$; vnde 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 numerorum 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 quaternarium est diuibilis, tum etiam quotus erit numerus eiusdem 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 $aa+3bb=4cc+12dd$, vnde, 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 diuisibilis per 4. Namque, cum tam $a+b$, quam $a-b$, sit numerus par, eorumque summa sit $2a$, hoc est numerus impariter par, necesse est, vt alter eorum sit impariter 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

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

vnde, 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 tam 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 quemcunque alium

alium primum formae $aa+3bb$; quotum scilicet inde oriundum pariter fore numerum eiusdem formae. Hunc in finem, vt 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, vt alteruter istorum factorum, scilicet vel $aq+bp$, vel $aq-bp$, sit per $pp+3qq$ diuisibilis. Ponatur ergo pro vtroque casu $aq\pm bp=m(pp+3qq)$; hincque fiet

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

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

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

Cum igitur numeri a et b necessario hoc modo expri-

 mantur,

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

$$aa+3bb=3mmpp+9mmqq+3nnqq+nnpp$$
$$=(pp+3qq)(nn+3mm)$$

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 $aa+3bb$ diviſorem 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

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

neque

neque hic amplius opus eſt, conditionem adieciſſe, vt $pp+3qq$ 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 quotcunque talium numerorum extenditur.

Scholion.

19. Etiamſi 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: tametſi 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 $(aq+bp)(aq-bp)$ fit diuifibile, alterutrum factorem diuifibilem effe debere per $pp+3qq$. Deinde vero etiam ex eo, quod p et q fint numeri inter fe primi, deriuauimus producti $p(mp\pm b)$, quod per q eft diuifibile, factorem $mp\pm b$ per q diuifibilem effe debere; quae pofterior conditio cum priore neceffario eft connexa.

Propofitio V.

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

Demonftratio.

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

Coroll. 1.

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

formae $pp+3qq$, et praeterea numero M, ita vt ſit $aa+3bb=MPQRS$, 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 aeque 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 diviſibiles, etiamſi 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 vtique duo adſunt factores N et N, quorum neuter in forma $pp+3qq$ continetur, vti §. 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 vllum 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 praebet factorem 4, quasi simplicem spectandum. Diligentius igitur examinandum restat, vtrum, dum a et b sunt primi inter se, numerus $aa + 3bb$ habeat vllum diuisorem 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 diuisor cuiuspiam numeri $aa + 3bb$, numeris a et b existentibus inter se primis, tum exhiberi posset alius numerus primus praeter binarium, minor B, in forma $pp + 3qq$ pariter non contentus, qui etiam futurus esset diuisor cuiuspiam numeri formae $aa + 3bb$, 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 diuisibilis ponitur, erunt ii quoque primi ad A. Si illi numeri essent maiores, quam A, statui posset $a = m\mathrm{A} \pm c$, et $b = n\mathrm{A} \pm d$, vt numeri c et d, qui pariter tum inter se, quam ad A, futuri essent primi, forent semissi ipsius A minores, scilicet $c < \frac{1}{2}\mathrm{A}$ et $d < \frac{1}{2}\mathrm{A}$, quia A, vt pote primus, est impar, casum enim quo $\mathrm{A} = 2$ hinc excipimus. Prodiret autem hac positione

$$aa + 3bb = mm\mathrm{AA} \pm 2m\mathrm{A}c + cc + 3nn\mathrm{AA} \pm 6n\mathrm{A}d + 3dd$$

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 hypothesin 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 inuolueret; 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 posset, 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 quamtumuis 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 distribuantur, quarum prior contineat eos, qui sunt formae $pp + 3qq$; posterior vero eos, qui ad hanc formam

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 pluribusue 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 quotcunque 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 assumsimus, numeros a et b esse primos inter se: sin autem non essent primi, sed maximum haberent diuisorem communem m, vt 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 inuoluet

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

Propositio VIII.

34. Omnis numerus primus formae $pp+3qq$, si per 6 diuidatur, relinquit vnitatem, 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, euidens est, nullos numeros primos posterioris formae $6n-1$, in forma $pp+3qq$ contineri.

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 $6n-1$ sit 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 $6n+1$ sit diuisibilis: in quo negotio loco formae $aa+3bb$ etiam haec $ff\pm fg+gg$ illi aequiualens accipi potest. Si enim numerum f et g alteruter, puta g, fuerit par, erit

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

sin

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

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

Quodſi ergo exhiberi queat numerus $ff \pm fg + gg$ 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 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:

$2^{2n}-1$; $3^{2n}-1$; $4^{2n}-1$; $5^{2n}-1$; ...... $(6n)^{2n}-1$; 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 exprimuntur:

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

vbi, cum ſit $2n+2<6n$, nullae poteſtates numerorum per $6n+1$ diuiſibilium ingrediuntur. Aliunde autem conſtat, differentiam ordinis $2n$ eſſe $=1.2.3.4\dots\dots 2n$, quae, cum certe non ſit per $6n+1$ diuiſibilis, manifeſto indicat, reperiri adeo inter hos numeros:

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

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 inueniendis tribus cubis, quorum summa sit cubus, assumseram, iam plane rigide sunt demonstrata. Assumseram autem primo, numeros formae $aa+3bb$, seu $ff\pm fg+gg$, 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 vsus 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 $a^n\pm b^n=c^n$ in rationalibus nunquam locum habere posse, statim atque exponens n binarium superet, nisi vnus numerorum a, b, c euanescat. Deinde etsi demonstraui, 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 aeque est certum, et a *Fermatio* demon-

stratum.

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 aeque 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-