DE NVMERIS QVI SVNT AGGREGATA DVORVM QVADRATORVM.

AVCT. L. EVLERO.

§. 1.

Naturam numerorum pluribus modis ſcrutari ſolent Arithmetici, dum eorum originem vel per additionem vel per multiplicationem repraeſentant. Prioris generis ſine dubio ſimpliciſſima eſt compoſitio ex vnitatibus, qua omnes numeri integri per aggregationem vnitatum oriri concipiuntur. Tum numeri quoque ita conſiderari poſſunt, prouti ex additione duorum pluriumue aliorum numerorum integrorum naſcuntur, quo pertinet problema de partitione numerorum, cuius ſolutionem aliquot abhinc annis expoſui, in quo quaeritur, quot variis modis quilibet numerus propoſitus per additionem duorum pluriumue numerorum minorum reſultare poſſit. Hic autem conſtitui eam numerorum compoſitionem perpendere, qua per additionem duorum quadratorum prodeunt; et cum hoc modo non omnes numeri oriantur, quoniam ingens eſt eorum multitudo, qui per additionem duorum quadratorum produci nequeunt, in eorum naturam et proprietates, qui ſunt ſummae duorum quadratorum, hic inquiram. Quarum proprietatum etiamſi pleraeque iam ſint cognitae, et quaſi per inductionem erutae, tamen firmis demonſtrationibus maximam partem deſtituuntur: quarum veritati cum haud contemnenda pars Analyſeos Diophanteae innitatur, in hac diſſertatione plurium huiusmodi propoſitionum, quae adhuc ſine demonſtrationibus ſunt admiſſae, demonſtrationes adornabo, ſimul vero etiam eas commemorabo, quas mihi quidem etiamnunc demonſtrare non licuit, etiamſi de earum veritate nullo modo dubitare queamus.

§. 2. Primum igitur cum numeri quadrati ſint: 0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, etc. iſtos numeros qui ex combinatione binorum quadratorum oriuntur, inſpexiſſe iuuabit, quos propterea vsque ad 200 hic apponam:

0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34, 36, 37, 40, 41, 45, 49, 50, 52, 53, 58, 61, 64, 65, 68, 72, 73, 74, 80, 81, 82, 85, 89, 90, 97, 98, 100, 101, 104, 106, 109, 113, 116, 117, 121, 122, 125, 128, 130, 136, 137, 144, 145, 146, 148, 149, 153, 157, 160, 162, 164, 169, 170, 173, 178, 180, 181, 185, 193, 194, 169, 197, 200 etc.

Hi nempe omnes ſunt numeri vsque ad 200, qui ex additione duorum quadratorum proueniunt: hosque numeros cum omnibus in infinitum ſequentibus vocabo ſummas duorum quadratorum, quos idcirco in hac formula generali $xx+yy$ comprehendi manifeſtum eſt, dum pro x et y ſucceſſiue omnes numeri integri 0, 1, 2, 3, 4, 5, 6 etc. ſubſtituuntur. Qui igitur numeri in his non reperiuntur, ii non ſunt ſummae duorum quadratorum, qui ergo

go sunt vsque ad 200:
3, 6, 7, 11, 12, 14, 15, 19, 21, 22, 23, 24, 27, 28, 30, 31, 33, 35, 38, 39, 42, 43, 44, 46, 47, 48, 51, 54, 55, 56, 57, 59, 60, 62, 63, 66, 67, 69, 70, 71, 75, 76, 77, 78, 79, 83, 84, 86, 87, 88, 91, 92, 93, 94, 95, 96, 99, 102, 103, 105, 107, 108, 110, 111, 112, 114, 115, 118, 119, 120, 123, 124, 126, 127, 129, 131, 132, 133, 134, 135, 138, 139, 140, 141, 142, 143, 147, 150, 151, 152, 154, 155, 156, 158, 159, 161, 163, 165, 166, 167, 168, 171, 172, 174, 175, 176, 177, 179, 182, 183, 184, 186, 187, 188, 189, 190, 191, 192, 195, 198, 199 etc.
Vnde patet saltem vsque ad 200 multitudinem numerorum qui non sunt summae duorum quadratorum, maiorem esse quam eorum qui sunt summae duorum quadratorum. Ceterum inspicienti statim patebit neutram istorum numerorum seriem certa et assignabili lege contineri; atque ob hoc ipsum difficilius erit vtriusque indolem inuestigare.

§. 3. Cum omnis numerus quadratus sit vel par, hocque casu per 4 diuisibilis et in hac forma $4a$ contentus, vel impar, hocque casu in hac forma $8b+1$ continеatur: omnis numerus ex duobus quadratis compositus erit vel 1mo. summa duorum quadratorum parium, et ad hanc formam $4a+4b$ pertinebit; eritque ergo per 4 diuisibilis.

Vel 2do. Summa duorum quadratorum alterius paris alterius imparis, et propterea in huiusmodi forma

$4a + 8b + 1$ seu in hac $4a + 1$ continebitur: vnitate ergo excedet multiplum quaternarii.

Vel 3tio. Summa duorum quadratorum imparium, eritque idcirco huius formae $8a + 1 + 8b + 1$ seu in hac $8a + 2$ continebitur. Erit scilicet numerus impariter par et binario excedet multiplum octonarii.

Quia ergo omnes numeri impares vel vnitate excedunt multiplum quaternarii seu huius sunt formae $4n + 1$ vel vnitate deficiunt a multiplo quaternarii seu huius sunt formae $4n - 1$; patet nullos numeros impares huius posterioris formae $4n - 1$ esse summas duorum quadratorum, seu ex serie numerorum qui sunt summae duorum quadratorum excluduntur omnes numeri in hac forma contenti $4n - 1$.

Deinde quia omnes numeri impariter pares vel binario superant multiplum octonarii, vt sint $8n + 2$, vel binario deficiunt a multiplo octonarii vt sint $8n - 2$, patet nullos numeros huius posterioris formae esse summas duorum quadratorum, sicque ex serie numerorum qui sunt summae duorum quadratorum excluduntur numeri huius formae $8n - 2$.

Interim tamen probe obseruandum est neque omnes numeros in hac forma $4n + 1$, neque in hac $8n + 2$ contentos esse summas duorum quadratorum. Illius enim formae excluduntur numeri: 21, 33, 57, 69, 77, 93, 105, 129, etc. huius vero isti: 42, 66, 114, 138, 154, etc. quorum ratio deinceps inuestigabitur. §. 4.

§. 4. Interim tamen numeri, qui ſunt ſummae duorum quadratorum ita nexu quodam inter ſe coniunguntur, vt ex vno huius indolis numero infiniti alii eiusdem naturae aſſignari queant. Quod quo facilius perſpiciatur, ſequentia lemmata, quae quidem vulgo ſatis ſunt nota, adiungam.

I. Si numerus p ſit ſumma duorum quadratorum, erunt quoque numeri $4p$, $9p$, $16p$ et generatim nnp ſummae duorum quadratorum.

Cum enim ſit $p = aa + bb$, erit $4p = 4aa + 4bb$; $9p = 9aa + 9bb$: $16p = 16aa + 16bb$ et $nnp = nnaa + nnbb$, quae formulae ſunt pariter ſummae duorum quadratorum.

II. Si numerus p ſit ſumma duorum quadratorum, erit quoque $2p$, et generatim $2nnp$ ſumma duorum quadratorum.

Sit enim $p = aa + bb$ erit $2p = 2aa + 2bb$. Sed eſt $2aa + 2bb = (a+b)^2 + (a-b)^2$, vnde erit $2p = (a+b)^2 + (a-b)^2$, ac propterea ſumma duorum quadratorum. Hinc vero porro erit $2nnp = nn(a+b)^2 + nn(a-b)^2$.

III. Si numerus par $2p$ fuerit ſumma duorum quadratorum, erit etiam eius ſemiſſis p ſumma duorum quadratorum.

Sit enim $2p = aa + bb$, erit numerorum a et b vterque vel par, vel impar. vnde vtroque caſu erit tam $\frac{a+b}{2}$ quam $\frac{a-b}{2}$ numerus integer. Eſt vero $aa + bb =$

$bb = 2\left(\frac{a+b}{2}\right)^2 + 2\left(\frac{a-b}{2}\right)^2$, quo valore ſubſtituto fit $p = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2$.

Hinc ergo omnes numeri pares, qui ſunt ſummae duorum quadratorum, per continuam biſectionem tandem reuocantur ad numeros impares eiusdem indolis. Quare viciſſim ſi ſoli numeri impares, qui ſunt ſummae duorum quadratorum cognoſcantur, ex iis omnes quoque pares per continuam duplicationem deriuabuntur.

§. 5. Deinde notatu dignum eſt ſequens theorema, quo natura numerorum, qui ſunt ſummae duorum quadratorum non mediocriter illuſtratur.

THEOR. *Si* p *et* q *ſint duo numeri, quorum vterque eſt ſumma duorum quadratorum, erit etiam eorum productum* pq *ſumma duorum quadratorum.*

DEM. Sit $p = aa + bb$ et $q = cc + dd$ erit $pq = (aa + bb)(cc + dd) = aacc + aadd + bbcc + bbdd$: quae expreſſio hoc modo repraeſentari poteſt vt ſit:

$pq = aacc + 2abcd + bbdd + aadd - 2abcd + bbcc$, ideoque $pq = (ac + bd)^2 + (ad - bc)^2$: vnde productum pq erit ſumma duorum quadratorum. Q. E. D.

Ex hac propoſitione ſequitur, quomodocunque plures numeri, qui ſinguli ſint ſummae duorum quadratorum inuicem multiplicentur, producta ſemper eſſe ſummas duorum quadratorum. Atque ex forma generali tradita patet, productum ex duobus huiusmodi numeris duplici modo in in duo quadrata resolui posse: si enim sit $p=aa+bb$, et $q=cc+dd$, erit tam $pq=(ac+bd)^2+(ad-bc)^2$, quam $pq=(ac-bd)^2+(ad+bc)^2$, quae formulae erunt diversae, nisi sit, vel $a=b$, vel $c=d$. Sic cum sit $5=1+4$, et $13=4+9$, productum $5.13=65$ duplici modo erit summa duorum quadratorum, scilicet erit $65=(1.3+2.2)^2+(2.3-1.2)^2=49+16$, et $65=(2.2-1.3)^2+(2.3+1.2)^2=1+64$. Atque si productum habeatur ex pluribus numeris, qui singuli sint summae duorum quadratorum, id pluribus modis in duo quadrata resolui poterit. Vti si proponatur numerus $1105=5.13.17$, eius resolutiones in duo quadrata erunt hae: $1105=33^2+4^2=32^2+9^2=31^2+12^2=24^2+23^2$. Quatuor scilicet hic resolutiones locum habent.

§. 6. Quanquam autem ita euictum est, si factores p et q sint summae duorum quadratorum, etiam fore productum pq summam duorum quadratorum; tamen huius propositionis conuersa hinc non sequitur, vt, si productum sit duorum quadratorum summa, etiam eius factores sint numeri eiusdem naturae, neque enim hanc conclusionem regulae Logicae, neque ipsa rei natura probarent. Nam numerus $45=36+9$ est summa duorum quadratorum, interim tamen horum factorum eius 3.15 neuter est summa duorum quadratorum. Magis autem firma videatur haec conclusio: si productum pq, et alteruter eius factor p fuerint duorum quadratorum summae, alterum quoque factorem q fore summam duorum quadratorum. Tametsi autem haec conclusio forte sit vera, regulis tamen ratiocinandi non confirmatur, neque enim cum demonstratum sit, si producti pq, bini factores p et q, sint duorum quadratorum summae, ipsum pq fore summam duorum quadratorum, hinc legitima consequentia inferri potest; si et productum pq, et alter factor p, sint summae duorum quadratorum, etiam alterum factorem q fore summam duorum quadratorum. Huiusmodi enim consequentiam non esse legitimam, vel hoc exemplum euidenter euincet: certum est si bini factores p et q sint numeri pares, etiam productum pq fore numerum parem, si quis autem hinc concludere velit, si productum pq et alter factor p sint numeri pares, etiam alterum factorem q fore parem, is vehementer falleretur.

§. 7. Quare si verum sit, vt, cum productum pq et alter eius factor p fuerint summae duorum quadratorum, alter quoque factor q sit summa duorum quadratorum; haec propositio non ex ante demonstrata potest inferri, sed peculiari demonstratione muniri debet. Haec autem demonstratio non tam plana est, quam praecedens, et non nisi per plures ambages concinnari potest, ac demonstratio quidem, quam inueni, ita comparata videtur, vt non mediocrem vim ratiocinii requirat. Hanc ob rem propositiones, ex quibus tandem non solum haec veritas conficitur, sed etiam aliae insignes proprietates huiusmodi numerorum, qui sunt summae duorum quadratorum, cognoscuntur, cum suis demonstrationibus hic ordine proponam, operamque dabo, vt nihil quicquam in rigore demonstrandi desiderari queat. Iis autem, quae hactenus de his numeris praemisi, vti sunt triuia et in vulgus nota, ita instar lemmatum in sequentibus demonstrationibus vtar.

PRO-

PROPOSITIO I.

§. 8. *Si productum* p q *sit summa duorum quadratorum, et alter factor* p *sit numerus primus, pariterque duorum quadratorum summa, erit quoque alter factor* q *summa duorum quadratorum.*

DEMONSTRATIO.

Sit $pq = aa + bb$, et $p = cc + dd$; quia p est numerus primus, erunt c et d numeri inter se primi. Erit itaque $q = \frac{aa+bb}{cc+dd}$, et propterea, ob q numerum integrum, numerator $aa + bb$ per denominatorem $cc + dd$ erit diuisibilis. Hinc quoque per $cc + dd$ diuisibilis erit numerus $cc(aa + bb) = aacc + bbcc$; at cum etiam hic numerus $aa(cc + dd) = aacc + aadd$ per $cc + dd$ sit diuisibilis, horum numerorum differentia $aacc + bbcc - aacc - aadd$ seu $bbcc - aadd$ per $cc + dd$ diuisibilis sit necesse est. Cum autem sit $cc + dd$ numerus primus, et $bbcc - aadd$ factores habeat $bc + ad$ et $bc - ad$, alteruter horum factorum, nempe $bc \pm ad$ per $cc + dd$ erit diuisibilis. Sit itaque $bc \pm ad = mcc + mdd$: quicunque autem numeri sint a et b, ii ita exprimi possunt, vt sit $b = mc + x$, et $a = \pm md + y$, existentibus x et y numeris integris siue affirmatiuis siue negatiuis. His vero valoribus pro b et a substitutis aequatio $bc \pm ad = mcc + mdd$ induet hanc formam: $mcc + cx + mdd \pm dy = mcc + mdd$ seu $cx \pm dy = 0$. Hinc erit $\frac{x}{y} = \mp \frac{d}{c}$, et quia d et c sunt numeri primi inter se, necesse est, vt sit $x = nd$ et $y = \mp nc$, vnde habebitur $a = \pm md \mp nc$ et $b =$

 $mc +$

$mc + nd$, huiusmodi ſcilicet valores habere debebunt numeri a et b, vt numerus $pq = aa + bb$ ſit diuiſibilis per numerum primum $p = cc + dd$. Verum iſtis valoribus pro a et b ſubſtitutis fiet:
$pq = mmdd - 2mncd + nncc + mmcc + 2mncd + nndd$, ſeu $pq = (mm + nn)(cc + dd)$. Iam ob $p = cc + dd$ erit $q = mm + nn$; ideoque ſi productum pq fuerit ſumma duorum quadratorum $aa + bb$, et alter factor p ſit numerus primus pariterque duorum quadratorum ſumma $cc + dd$, neceſſario ſequitur etiam alterum factorem q fore ſummam duorum quadratorum. Q. E. D.

COROLL. 1.

§. 9. Si ergo ſumma duorum quadratorum diuiſibilis ſit per numerum primum, qui ipſe ſit ſumma duorum quadratorum, etiam quotus ex diuiſione reſultans erit ſumma duorum quadratorum. Ita ſi ſumma duorum quadratorum fuerit diuiſibilis per quempiam ex his numeris primis 2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97 etc. quotus ſemper erit ſumma duorum quadratorum.

COROLL. 2.

§. 10. Si ergo litterae α, β, γ, δ, etc. denotent huiusmodi numeros primos, qui ſunt ſummae duorum quadratorum; hinc patet, ſi productum αq ſit ſumma duorum quadratorum, fore etiam factorem q ſummam duorum quadratorum.

COROLL.

COROLL. 3.

§. 11. Hinc autem porro facile colligitur, ſi productum $\alpha \beta q$ fuerit ſumma duorum quadratorum, fore etiam factorem q ſummam duorum quadratorum. Cum enim ſit $\alpha \beta q$ ſumma duorum quadratorum, per *coroll. praec.* erit quoque βq ſumma duorum quadratorum; et ob eandem rationem erit quoque q ſumma duorum quadratorum.

COROLL. 4.

§. 12. Simili modo euidens eſt, ſi productum $\alpha \beta \gamma \delta \varepsilon q$ fuerit ſumma duorum quadratorum, tum quoque factorem q eſſe ſummam duorum quadratorum; hinc ſi productum pq ſit ſumma duorum quadratorum, eiusque factor p productum ex quotcunque numeris primis, quorum ſinguli ſint ſummae duorum quadratorum, fore etiam alterum factorem q ſummam duorum quadratorum.

SCHOLION.

§. 13. Regulae Logicae non permittunt, vt haec propoſitio ita conuertatur, vt, quoties alter factor q ſit ſumma duorum quadratorum, etiam alter factor p pronunciari poſſit, vel ſumma duorum quadratorum, ſi eſt primus, vel productum ex numeris primis, qui ſinguli ſint ſummae duorum quadratorum. De hoc ipſo enim nondum conſtat, vtrum productum ex aliquot numeris primis, qui ipſi non ſint ſummae duorum quadratorum, nequeat eſſe ſumma duorum quadratorum: quin potius contrario iam habemus caſum, quo productum $45 = 3 \cdot 3 \cdot 5$ est ſumma duorum quadratorum, cum tamen eius factores 3 et 3 non ſint huius indolis. Verum propoſitio *coroll. vlt.* ita conuerti poteſt, vt a negatione conſequentis recte ad negationem antecedentis concludatur, quam conuerſionem vtpote maximi momenti in hac propoſitione complectar.

PROPOSITIO II.

§. 14. *Si productum* pq *ſit ſumma duorum quadratorum, eius factor autem* q *non ſit ſumma duorum quadratorum, tum alter factor* p, *ſi ſit numerus primus, non erit ſumma duorum quadratorum, ſin autem non ſit primus, ſaltem factorem certe habebit primum, qui non ſit ſumma duorum quadratorum.*

DEMONSTRATIO.

Cum alter factor p ſit, vel numerus primus, vel compoſitus, vtrumque caſum ſeorſim perpendere conuenit. Sit 1mo p numerus primus; cum igitur ſi eſſet ſumma duorum quadratorum; quoque alter factor q foret ſumma duorum quadratorum; quod cum hypotheſi aduerſetur, ſequitur, factorem p non eſſe ſummam duorum quadratorum. Sit 2do p numerus compoſitus; et ex praec. liquet, ſi omnes eius factores primi eſſent ſummae duorum quadratorum, etiam alterum factorem q eiusdem fore indolis. Quare cum per hypotheſin q non ſit ſumma duorum quadratorum, ſequitur, non omnes factores ipſius p eſſe ſummas duorum quadratorum. Q. E. D.

COROLL.

COROLL. 1.

§. 15. Si igitur productum pq ſit ſumma duorum quadratorum, eius tamen alter factor q in duo quadrata ſit irreſolubilis; alter factor p, vel ipſe non erit ſumma duorum quadratorum, vel ſaltem factorem habebit primum in duo quadrata irreſolubilem. Vti ſi ſit $pq = 45$ et $q = 3$, erit $p = 15$ et factorem habet 3, qui non eſt ſumma duorum quadratorum.

COROLL. 2.

§. 16. Hinc autem nondum concludere licet, alterum factorem p plane non eſſe ſummam duorum quadratorum, quamuis enim hoc certum ſit caſu, quo p eſt numerus primus, tamen id nondum conſtat caſu, quo p eſt numerus compoſitus; quia p habere poſſet factorem in duo quadrata irreſolubilem, etiamſi ipſe numerus p eſſet ſumma duorum quadratorum.

COROLL. 3.

§. 17. Hoc autem colligere licet; ſi p eſſet ſumma duorum quadratorum, tum non ſolum vnum, ſed ad minimum duos habere debere factores primos in duo quadrata irreſolubiles. Sit enim $p = \alpha \beta \gamma \delta$, et δ factor ille in duo quadrata irreſolubilis; perſpicuum eſt, ſi p eſſet ſumma duorum quadratorum, deleto factore δ, inſuper factorem reſiduum $\alpha \beta \gamma$ factorem in duo quadrata irreſolubilem habere debere.

SCHOLION.

§. 18. Cum de diuiſoribus numerorum, qui ſunt ſummae duorum quadratorum, quaeſtio inſtituitur, circa quadratorum ſummam $aa + bb$, caſus hi probe ſunt diſtinguendi, vtrum haec quadrata aa et bb, ſeu eorum radices a et b ſint numeri primi inter ſe nec ne? Si enim a et b non ſint numeri primi inter ſe, ſed habeant communem diuiſorem n, vt ſit $a = nc$ et $b = nd$, ſumma quadratorum erit $nncc + nndd = nn(cc + dd)$, ac propterea diuiſorem habebit n, hoc eſt, numerum quemcunque. Sin autem radices a et b fuerint numeri primi inter ſe, tum ſumma quadratorum $aa + bb$ plures numeros pro diuiſoribus non admittet; euidens enim eſt huiusmodi ſummam duorum quadratorum $aa + bb$ nunquam per 3 eſſe diuiſibilem. Nam quia per hypotheſin vtrumque quadratum ſeorſim non eſt per 3 diuiſibile, cum alioquin non forent prima inter ſe; ſi ſumma $aa + bb$ eſſet per 3 diuiſibilis, neutrum foret per 3 diuiſibile. Vtriusque ergo radices futurae eſſent, vel huius formae $3m + 1$, vel huius $3m - 1$; ſed ſumma huiusmodi duorum quadratorum, per 3 diuiſa, ſemper reſiduum 2 relinquit, ideoque per 3 nunquam eſt diuiſibilis. Eodem modo intelligitur, ſummam duorum quadratorum inter ſe primorum $aa + bb$ nunquam eſſe per 7, vel 11, vel 19 etc. diuiſibilem. Quinam autem ſint in genere hi numeri, qui nunquam ſummae duorum quadratorum inter ſe primorum diuiſores exiſtere queant, hoc modo non facile definitur. Demonſtrari igitur conuenit propoſitionem alias quidem ſatis notam, ſummam duorum quadratorum inter ſe primorum alios diuiſores primos

primos non admittere, nisi qui ipsi sint summae duorum quadratorum. Praemitti autem debet sequens propositio.

PROPOSITIO III.

§. 19. *Si summa duorum quadratorum inter se primorum* $aa + bb$ *diuisibilis sit per numerum* p, *semper exhiberi poterit summa duorum aliorum quadratorum* $cc + dd$ *diuisibilis per eundem numerum* p, *ita vt ista summa* $cc + dd$ *non sit maior quam* $\frac{1}{2}pp$.

DEMONSTRATIO.

Sit summa duorum quadratorum inter se primorum $aa + bb$ diuisibilis per numerum p, et a et b numeri quantumuis magni. Quia ergo neque a neque b seorsim per p diuisibilis est, numeri a et b ita exprimi poterunt, vt sit $a = mp \pm c$ et $b = np \pm d$, vbi numeros m et n ita determinare licet, vt c et d non excedant semissem ipsius p. Erit ergo $aa + bb = mmpp \pm 2mcp + cc + nnpp \pm 2ndp + dd$, quae formula cum et tota diuisibilis sit per p (per hyp.) et eius pars $mmpp \pm 2mcp + nnpp \pm 2ndp$ per se diuisorem habeat p, necesse est, vt altera pars $cc + dd$, quae est summa duorum quadratorum, itidem per p sit diuisibilis. At cum radices c et d non excedant semissem ipsius p, summa quadratorum $cc + dd$ non excedet quadratum $\frac{1}{4}pp$ bis sumtum; ideoque summa duorum quadratorum $cc + dd$ exhiberi potest non maior quam $\frac{1}{2}pp$, quae tamen sit per p diuisibilis. Q. E. D.

COROLL. 1.

§. 20. Si igitur non detur ſumma duorum quadratorum inter ſe primorum diuiſibilis per numerum p, quae non excedat $\frac{1}{2}pp$, nullae omnino dantur ſummae duorum quadratorum inter ſe primorum, quae per hunc numerum p eſſent diuiſibiles.

COROLL. 2.

§. 21. Sic cum nulla detur ſumma duorum quadratorum inter ſe primorum infra $\frac{1}{2}\cdot 3^2$ ſeu infra $4\frac{1}{2}$, quae ſit per 3 diuiſibilis, hinc luculenter ſequitur, nullam omnino ſummam duorum quadratorum inter ſe primorum per 3 eſſe diuiſibilem. Similique modo pro numero 7, cum non detur ſumma duorum quadratorum infra $\frac{1}{2}7^2 = 24\frac{1}{2}$ per 7 diuiſibilis, ſequitur ne in maximis quidem numeris dari ſummas duorum quadratorum inter ſe primorum per 7 diuiſibiles.

PROPOSITIO IV.

§. 22. *Summa duorum quadratorum inter ſe primorum diuidi nequit per vllum numerum, qui ipſe non ſit ſumma duorum quadratorum.*

DEMONSTRATIO.

Ad hoc demonſtrandum ponamus ſummam duorum quadratorum inter ſe primorum $aa + bb$ diuiſibilem eſſe per numerum p, qui non ſit ſumma duorum quadratorum. Exhiberi ergo poſſet alia ſumma duorum qua-

quadratorum inter se primorum $cc + dd$ non maior quam $\frac{1}{2}pp$, quae esset diuisibilis per p. Sit igitur $cc + dd = pq$, et cum p non sit summa duorum quadratorum, vel ipse numerus q non erit eiusmodi summa, vel saltem factorem habebit r, qui non erit summa duorum quadratorum. Quia vero $pq < \frac{1}{2}pp$, erit $q < \frac{1}{2}p$ et multo magis $r < \frac{1}{2}p$. Quare cum $cc + dd$ quoque diuisibilis sit per $r < \frac{1}{2}p$; per *prop. praec.* summa duorum quadratorum $ee + ff$ per eundem numerum r diuisibilis exhiberi posset, quae non excederet $\frac{1}{2}rr$, neque multo magis $\frac{1}{8}pp$. Et cum r non sit summa duorum quadratorum; simili modo procedendo continuo ad minores summas duorum quadratorum deueniretur, quae per numerum non summam duorum quadratorum essent diuisibiles. Quocirca cum in minimis numeris nulla detur summa duorum quadratorum inter se primorum, quae esset diuisibilis per numerum, qui non sit summa duorum quadratorum, ne in maximis quidem numeris eiusmodi erunt summae duorum quadratorum, quae diuisibiles sint per numeros, qui ipsi non essent summae duorum quadratorum. Q. E. D.

COROLL. 1.

§. 23. Si ergo summa duorum quadratorum inter se primorum non fuerit numerus primus, omnes eius factores primi quoque erunt summae duorum quadratorum. Quemadmodum igitur productum ex quotcunque numeris primis, qui ipsi sunt summae duorum quadratorum, pariter est summa duorum quadratorum, ita nunc huius propositionis conuersa est demonstrata, vt summa duorum quadratorum (inter ſe primorum) per multiplicationem oriri nequeat, niſi ex numeris, qui ipſi ſint ſummae duorum quadratorum.

COROLL. 2.

§. 24. Omnes ergo numeri, qui ſunt ſummae duorum quadratorum inter ſe primorum, vel ipſi in hac ſerie numerorum primorum continentur:
2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, etc. vel ex duobus pluribusue numeris huius ſeriei per multiplicationem componuntur. Omnes autem hi numeri primi praeter 2 vnitate excedunt multiplum quaternarii ſeu in hac forma $4n+1$ continentur.

COROLL. 3.

§. 25. Si igitur ſumma duorum quadratorum $aa+bb$ diuiſibilis ſit per numerum, qui non fuerit ſumma duorum quadratorum; hinc intelligetur quadrata illa aa et bb non eſſe inter ſe prima, neque adeo eorum radices a et b.

COROLL. 4.

§. 26. Cum autem ſi $a=nc$ et $b=nd$ ſumma duorum quadratorum $aa+bb=nn(cc+dd)$ per quemuis numerum n, qui non eſt ſumma duorum quadratorum, diuidi poſſit, quoniam non ſolum per n, ſed etiam per nn eſt diuiſibilis, euidens eſt, ſi ſumma duorum quadratorum diuiſibilis ſit per quempiam numerum, qui non eſt ſumma duorum quadratorum, tum eam quoque per quadratum huius numeri fore diuiſibilem. Sic cum $45=36+9$ ſit diuiſib. per 3, ſimul quoque diuiſibilis eſt per 9.

COROLL.

COROLL. 5.

§. 27. Cum nullus numerorum in hac forma $4n-1$ contentorum ſit ſumma duorum quadratorum, manifeſtum quoque eſt, nullam ſummam quadratorum inter ſe primorum diuidi poſſe per vllum numerum primum, in forma $4n-1$ contentum, qui numeri primi ſunt: 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107 etc.

SCHOLION.

§. 28. Cum omnes numeri primi, qui ſunt ſummae duorum quadratorum, excepto binario, hanc ſeriem conſtituant:

5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, etc.

qui non ſolum in hac forma $4n+1$ continentur, ſed etiam, quantumuis ea longe continuetur, deprehendemus in ea omnes omnino numeros primos huius formae $4n+1$ occurrere: vnde per inductionem ſatis probabiliter concludere licet, nullum dari numerum primum formae $4n+1$, qui non ſimul ſit ſumma duorum quadratorum. Interim tamen cum inductio quantumuis ampla vicem demonſtrationis ſuſtinere nequeat; hanc veritatem, quod omnis numerus primus formae $4n+1$ ſimul ſit ſumma duorum quadratorum, etiamſi nemo agnoſcere dubitet, tamen adhuc demonſtratis matheſeos veritatibus annumerare non licet. *Fermatius* quidem profeſſus eſt, ſe eius demonſtrationem inueniſſe; quia autem eam nusquam publicauit, aſſerto quidem huius profundiſſimi Viri merito fidem adhibemus, iſtamque numerorum proprietatem credimus; haecque cognitio noſtra mera fide ſine ſcientia nititur. Quanquam autem ego multum in demonſtratione eruenda fruſtra laboraui, tamen aliud argumentum pro hac veritate adſtruenda reperi, quod etiamſi non ſummum rigorem ſuſtineat, tamen cum inductione coniunctum demonſtrationi pene rigoroſae aequiualere videtur.

PROPOSITIO V.

§. 28. *Omnis numerus primus, qui vnitate excedit multiplum quaternarii, eſt ſumma duorum quadratorum.*

TENTAMEN DEMONSTRATIONIS.

Numeri primi, de quibus hic ſermo eſt, in hac forma $4n+1$ continentur. Quodſi ergo numerus $4n+1$ fuerit primus, demonſtraui per eum ſemper diuiſibilem eſſe hanc formam $a^{4n}-b^{4n}$, quicunque numeri pro a et b ſubſtituantur, dummodo neuter ſeorſim fuerit per $4n+1$ diuiſibilis. Cum autem ſit $a^{4n}-b^{4n}=(a^{2n}-b^{2n})(a^{2n}+b^{2n})$, neceſſe eſt, vt alteruter factor, nempe vel $a^{2n}-b^{2n}$, vel $a^{2n}+b^{2n}$ ſit diuiſibilis per numerum primum $4n+1$. Prout autem pro a et b alii atque alii numeri aſſumuntur, aliis caſibus formula $a^{2n}-b^{2n}$, aliis vero formula $a^{2n}+b^{2n}$ erit per $4n+1$ diuiſibilis: vnde aſſumere licet, etſi quidem hoc nondum firma demonſtratione euincere valeo, ſemper eiusmodi numeros pro a et b aſſignari poſſe, vt formula $a^{2n}-b^{2n}$ non ſit per $4n+1$ diuiſibilis: iis ergo caſibus altera formula $a^{2n}+b^{2n}$ neceſſario per $4n+1$ erit diuiſibilis. Sit $a^n=p$ et $b^n=q$, habebitur biturque summa duorum quadratorum $pp + qq$ per $4n + 1$ diuisibilis, ita vt neutrum quadratum pp vel qq seorsim habeat diuisorem $4n + 1$. Ideoque etiamsi fortasse pp et qq communem habeant diuisorem mm, vt sit $pp + qq = mm(rr + ss)$, quia factor communis mm diuisorem non habet $4n + 1$, necesse est, vt summa duorum quadratorum inter se primorum $rr + ss$ habeat diuisorem $4n + 1$; Consequenter cum huiusmodi summa duorum quadratorum alios non admittat diuisores, nisi qui ipsi sint summae duorum quadratorum, necesse est, vt numerus primus $4n + 1$ sit summa duorum quadratorum.

COROLL. 1.

§. 29. Demonstratio haec igitur esset perfecta, si modo demonstrari posset, semper eiusmodi existere valores pro a et b substituendos, quibus formula $a^{2n} - b^{2n}$ non fiat diuisibilis per numerum primum $4n + 1$; iisdem enim casibus formula $a^{2n} + b^{2n}$ necessario est diuisibilis per $4n + 1$.

COROLL. 2.

§. 30. Quod si quis autem hanc rem per calculum tentet, non modo semper plures casus, imo infinitos, formulae $a^{2n} - b^{2n}$ reperiet, quibus ea per numerum primum $4n + 1$ non est diuisibilis, sed etiam pro b vnitatem ponere licet, ita, vt etiam haec formula simplicior $a^{2n} - 1$ saepe numero per $4n + 1$ non sit diuisibilis.

SCHOLION

SCHOLION.

§. 31. Casus seu valores ipsius a, quibus formula $a^{2n}-1$ certe fit diuisibilis per numerum primum $4n+1$, facile assignari possunt. Primo enim si sit $a=pp$, formula $a^{2n}-1=p^{4n}-1$ semper est diuisibilis per $4n+1$, dummodo p non sit $=4n+1$ vel eius multiplo. Deinde si $a=pp\pm(4n+1)q$, formula $a^{2n}-1$ quoque diuisorem habet $4n+1$, resoluitur enim $a^{2n}=(pp\pm(4n+1)q)^{2n}$ in seriem terminorum, quorum primus est p^{4n}, sequentes vero omnes sponte sunt per $4n+1$ diuisibiles. Vnde patet, valores idoneos pro a esse omnia residua, quae restant, si numeri quadrati p^2 per $4n+1$ diuidantur. Haec autem residua siue pro a ponatur r, siue $4n+1+r$, siue $(4n+1)q+r$ prodeunt eadem, vnde omnia possibilia residua obtinentur, si pro p successiue statuantur numeri $1, 2, 3, 4, 5, \ldots$ vsque ad $4n$, at valor $4n$ pro p positus idem dat residuum, quod valor 1, similique modo valores 2 et $4n-1$, item 3 et $4n-2$, item 4 et $4n-3$ etc. eadem dant residua. Vnde cum bina semper residua, quae ex numeris $1, 2, 3, \ldots$ vsque ad $4n$ pro radicibus quadratorum sumtis proueniunt, sint aequalia, numerus diuersorum residuorum resultantium tantum erit $2n$, ideoque totidem dabuntur numeri ipso $4n+1$ minores, qui non esse possunt residua ex diuisione numerorum quadratorum per $4n+1$ emergentia; hique numeri pro a substituti semper formulam $a^{2n}-1$ reddent non diuisibilem per $4n+1$. Hoc quidem pariter demonstrari nequit; verumtamen quia periculum faciendo, quotcunque etiam numeri hoc modo explorentur, ne unicus quidem casus occurret, quo haec regula

gula fallat, eius veritatem agnoſcere oportet. Quo haec clarius perſpiciantur, exempla aliquot ſubiungam, ſit primo $4n+1=5$, et caſus, quibus formula a^2-1 per 5 erit diuiſibilis, habebuntur, ſi pro a reſidua ex diuiſione quadratorum per 5 oriunda ponantur, quae reſidua ſunt 1, 4. At ſi pro a ponatur vel 2, vel 3, formula a^2-1 non erit per 5 diuiſibilis; his ergo caſibus formula a^2+1 diuiſorem habebit 5. Deinde ſi ſit $4n+1=13$, ſeu $n=3$, reſidua, quae ex diuiſione numerorum quadratorum per 13 reſtant, ſunt 1, 4, 9, 3, 12, 10. vnde ſi quis numerorum reliquorum, 2, 5, 6, 7, 8, 11, pro a ſubſtituatur, non formula a^6-1, ſed a^6+1 per 13 erit diuiſibilis. Porro ſi $4n+1=17$, ſeu $n=4$, quia reſidua quadratorum per 17 diuiſorum ſunt 1, 4, 9, 16, 8, 2, 15, 13, ſi pro a ſtatuatur quiſpiam ex reliquis numeris 3, 5, 6, 7, 10, 11, 12, 14, non formula a^8-1, ſed haec a^8+1 erit per 17 diuiſibilis. Cum igitur haec lex perpetuo obſeruetur, haec inductio vim demonſtrationis fere induere cenſenda erit; hincque propoſitio tantopere confirmata videtur, vt eius veritatem non amplius in dubium vocare liceat. Interim tamen operae pretium eſſet eo maius, ſi quis rigoroſam huius propoſitionis demonſtrationem exhibere poſſet, quo magis de eius veritate ſimus certi: nullum enim eſt dubium, quin eiusmodi demonſtratio, tamdiu fruſtra quaeſita, ad plurimas alias inſignes numerorum proprietates ſit manuductura. Quamquam autem huius propoſitionis veritas extra dubium eſt poſita, tamen eas conſequentias, quae ipſi innituntur, diligenter notabo, ab aliisque, quae rigidis demonſtrationibus muniuntur, diſtinguam: ex hac autem propoſitione nondum demonſtrata ſequuntur haec corollaria, quae hoc nomine notata velim.

COROLL. 3.

§. 32. Si igitur numerus formae $4n+1$ in duo quadrata nullo modo reſolui nequeat, hoc certum erit ſignum, eum numerum non eſſe primum: ſi enim iſte numerus $4n+1$ eſſet primus, certe in duo quadrata reſolui poſſet. Sic cum numeri 21, 33, 57, 69, 77, 93 etc. qui in forma $4n+1$ continentur, non ſint ſummae duorum quadratorum, ex hoc ipſo patet, eos non eſſe primos.

COROLL. 4.

§. 33. In ſerie ergo numerorum, qui ſunt ſummae duorum quadratorum, omnes primo continentur numeri primi huius formae $4n+1$, deinde omnia producta ex duobus pluribusue huiusmodi numeris primis; tam producta ex ſingulis hisce numeris in binarium et quosuis numeros quadratos.

COROLL. 5.

§. 34. Omnes numeri n, ex quibus formula $4n+1$ euadit numerus primus, ſunt ſummae duorum numerorum trigonalium. Cum enim $4n+1$ ſit ſumma duorum quadratorum, erit eius duplum $8n+2$ ſumma duorum quadratorum imparium: ſit ergo $8n+2=(2x+1)^2+(2y+1)^2$, fiet $n=\frac{xx+x}{2}+\frac{yy+y}{2}$. Quare ſi n non ſit ſumma duorum numerorum trigonalium, certe numerus $4n+1$ non erit primus.

PRO-

PROPOSITIO VI.

§. 35. *Si numerus formae* $4n+1$ *vnico modo in duo quadrata inter se prima resolui queat, tum certe est numerus primus.*

DEMONSTRATIO.

Quoniam enim hic numerus est summa duorum quadratorum inter se primorum, si non sit prima, singuli eius factores erunt summae duorum quadratorum. Quare si hic numerus non esset primus, in huiusmodi saltem duos factores resolui posset, vt esset $4n+1 = (aa+bb)(cc+dd)$, hoc autem casu duplex resolutio in duo quadrata locum habet; scilicet:

I. $4n+1 = (ac+bd)^2 + (ad-bc)^2$

II. $4n+1 = (ad+bc)^2 + (ac-bd)^2$

Haeque resolutiones semper sunt diuersae, nisi sit vel $ac+bd = ad+bc$ vel $ac+bd = ac-bd$. Priori vero casu foret $ac+bd-ad-bc=0$, seu $(a-b)(c-d)=0$, ideoque vel $a=b$ vel $c=d$; atque hinc vel $aa+bb$ vel $cc+dd$ numerus par, quorum neutrum esse potest diuisor ipsius $4n+1$ vtpote numeri imparis. Posteriori vero casu esset vel $b=0$ vel $d=0$, ideoque $4n+1$ vel $= aa(cc+dd)$ vel $= cc(aa+bb)$; vnde haec duo quadrata non forent prima inter se contra hypothesin. Quibus casibus notatis sequitur, numerum compositum $4n+1$, si in duo quadrata inter se prima fuerit resolubilis, eundem ad minimum duobus modis in duo quadrata esse resolubilem. Quo circa si tan-

 tum

tum vnico modo numerus $4n+1$ ſit ſumma duorum quadratorum, certe non erit compoſitus, ac per conſequens erit primus. Q. E. D.

COROLL. 1.

§. 36. Si igitur propoſito quopiam numero formae $4n+1$ poſt inſtitutum examen comperiatur, eum vnico modo in duo quadrata inter ſe prima reſolui poſſe, inde tuto colligemus, eum numerum eſſe primum; etiamſi eius diuiſibilitatem per numeros primos more conſueto non tentauerimus. Sic cum numerus 73 vnico modo ſit ſumma duorum quadratorum, nempe $64+9$, eum eſſe primum, certo nouimus.

COROLL. 2.

§. 37. Si ergo methodus expedita haberetur, cuius ope facile inquirere liceret, an et quot modis propoſitus numerus in forma $4n+1$ contentus in duo quadrata reſolui poſſit exinde promte iudicare poterimus, vtrum ſit primus; ſi enim vnico modo in duo quadrata ſit reſolubilis, eaque quadrata fuerint prima inter ſe, is certe pro primo erit habendus.

COROLL. 3.

§. 38. Manifeſtum autem eſt, ſi duo quadrata, in quae numerus quiſpiam reſoluitur, non ſint prima inter ſe, eum numerum non eſſe primum. Si enim numerus propoſitus inueniatur eſſe $= nnaa + nnbb$, tum diuiſores habebit n et nn: quod idem eſt intelligendum, ſi

numerus

numerus propofitus ipfe fit quadratum, feu $= aa + 0$, tum enim diuiforem habebit a.

SCHOLION.

§. 39. Haec regula numeros primos explorandi tantum ad numeros impares formae $4n + 1$ eft adftricta, numeri enim pares quandoque vnico modo in duo quadrata refolui poffunt, cum tamen non fint primi; ita 10 vnico modo eft fumma duorum quadratorum, etfi non eft primus, cuius rei ratio eft, quod in producto $(aa + bb)(cc + dd)$, cui huiusmodi numeri aequantur, eft vel $a = b$ vel $c = d$, quo cafu duplex refolutio, quae generatim innui videtur, ad vnam redit, vti in demonftratione eft animaduerfum. Neque vero hac exceptione regula data infringitur, cum numerorum parium per fe facile fit iudicium. Numeri autem impares alterius formae $4n - 1$ hinc fponte excluduntur, quoniam ii plane non in duo quadrata funt refolubilis. De cetero fi numerus $4n + 1$ vel plane non refolubilis fit in duo quadrata, vel pluribus modis haec refolutio fuccedat, pro priori cafu iam notauimus, eum numerum certe non effe primum, etfi hoc nititur *Prop. praec.* non fatis rigide demonftrata. Pro cafu vero pofteriori in fequenti propofitione iudicium afferetur.

PROPOSITIO VII.

§. 40. *Qui numerus duobus pluribusue diuerfis modis in duo quadrata refolui poteft, ille non eft primus, fed ex duobus ad minimum factoribus compofitus.*

DEMONSTRATIO.

Sit numerus propositus N, qui duplici modo in duo quadrata sit resolubilis; nempe $N = aa + bb = cc + dd$. Quoniam haec quadrata non sunt aequalia, alioquin enim numerus N per se non esset primus, sit $a > b$ et $c > d$, et quia resolutiones hae duae sunt diversae, neque erit $a = c$ neque $b = d$. Sit igitur $a > c$; erit $b < d$; vnde ponatur $a = c + x$ et $d = b + y$. Quare ob $aa + bb = cc + dd$ fiet: $2cx + xx = 2by + yy$. Sit vtraque forma $= xyz$, quia altera per x, altera per y est diuisibilis; fiet $x = \frac{yz - x}{2}$; $b = \frac{xz - y}{2}$; $a = \frac{yz + x}{2}$; $d = \frac{xz + y}{2}$ hincque erit $N = aa + bb = \frac{xxzz + yy + yyzz + xx}{4}$ seu $N = \frac{(yy + xx)(1 + zz)}{4}$. Nisi ergo $xx + yy$ per 4 sit diuisibile, erit $xx + yy$ diuisor ipsius N, sin autem $xx + yy$ sit per 4 diuisibile, vel numerus vtcunque compositus, eius certe factor quidam erit diuisor ipsius N. Cum igitur sit $x = a - c$ et $y = d - b$, numerus propositus $N = aa + bb = cc + dd$ diuisorem habebit vel ipsum numerum $(a - c)^2 + (d - b)^2$, vel eius semissem quadrantemue, et quia numeros a, b et c, d, inter se vtcunque permutare licet, factores ipsius N quoque erunt $(a - d)^2 + (c - b)^2$, vel etiam quia radices a, b, c, d negatiue assumere licet $(a \pm c)^2 + (d \pm b)^2$ vel $(a \pm d)^2 + (c \pm b)^2$, seu harum formularum semisses aliaeue partes aliquotae. Quare cum numeri plus vno modo in duo quadrata resolubilis factores adeo assignari possint, ille numerus certe non erit primus, sed compositus. Q. E. D.

COROLL.

COROLL. 1.

§. 41. Cum igitur numerus $N = aa + bb = cc + dd$ sit compositus, erit huiusmodi $N = (pp + qq)(rr + ss)$. Hinc autem viciſſim duplex reſolutio in duo quadrata reſultat, erit nempe:

$$a = pr + qs \quad \text{et} \quad c = ps + qr$$
$$b = ps - qr \qquad\quad d = pr - qs.$$

Hincque vlterius obtinetur $a - d = 2qs$ et $c - b = 2qr$, vnde fit $\frac{r}{s} = \frac{c-b}{a-d}$. Quare ſi fractio $\frac{c-b}{a-d}$ ad minimos terminos reducatur, vt ſit $\frac{c-b}{a-d} = \frac{r}{s}$, ex hac fractione $\frac{r}{s}$ orietur numeri N diuiſor $= rr + ss$, niſi ſit par, nam ſi fuerit par, eius dimidium ſumi debet.

COROLL. 2.

§. 42. Simili modo cum numeros a, b et c, d inter ſe permutare atque adeo negatiuos ponere liceat, ſi fractionum harum $\frac{a \pm c}{b \pm d}$, vel $\frac{a \pm d}{b \pm c}$ altera ad minimos terminos reducatur, vt fiat $= \frac{r}{s}$, erit $rr + ss$ ſemper diuiſor numeri propoſiti N.

COROLL. 3.

§. 43. Quanquam autem hinc plures duobus diuiſores naſci videntur, tamen diuerſae formulae ita ad eundem diuiſorem deducunt, vt non plures quam duo eliciantur, ſi quidem numerus propoſitus duobus tantum modis in duo quadrata fuerit reſolubilis. Sit, ſi $N = 85 = 9^2 + 2^2 = 7^2 + 6^2$; formulae $\frac{9 \pm 7}{6 \pm 2}$; $\frac{9 \pm 6}{7 \pm 2}$ has

qua-

quatuor tantum fractiones in minimis terminis ſuppeditant nempe : $\frac{2}{1}$; $\frac{4}{1}$; $\frac{5}{3}$; $\frac{3}{1}$; quarum binae poſteriores pro formula $rr + ss$ duplum valorem tantum exhiberit, eius qui ex primis oritur : vnde patebit, factores eſſe binos $2^2 + 1 = 5$ et $4^2 + 1 = 17$. Breuiſſime ergo hi factores inueniuntur, ſi tantum radices quadratorum pares et impares ſeorſim inuicem combinentur, et combinatio parium cum imparibus penitus omittatur, quia hinc fractiones orirentur, numeratorem et denominatorem impares habentes.

PROBLEMA.

§. 44. *Propoſito numero quocunque formae* $4n + 1$ *explorare vtrum primus ſit nec ne?*

SOLVTIO.

Per operationem deinceps explicandam inueſtigetur numerus propoſitus, vtrum in duo quadrata reſolui poſſet nec ne? et, ſi poſſit, an plus vno modo reſolutio ſuccedat? Si enim reſolutionem in duo quadrata plane non admittat, id per §. 32 certum erit ſignum, numerum propoſitum non eſſe primum, etiamſi haec concluſio ex *Prop. V.* non ſatis demonſtrata ſequatur. Hoc quidem caſu de eius diuiſoribus nihil conſtat; interim tamen certo colligimus, eum diuiſores primos habere formae $4m - 1$, quia ſi omnes eius factores eſſent formae $4m + 1$, is certe in duo quadrata foret reſolubilis. At ſi numerus propoſitus vnico modo ſit in duo quadrata reſolubilis, tum infallibiliter pro primo erit habendus. Sin autem

autem resolutio plus vno modo succedat, tum non solum constabit, eum non esse primum, sed etiam eius diuisores assignari poterunt per §. 43. His perpensis regulam tradam, cuius ope resolubilitas in duo quadrata non difficulter explorari poterit.

Numerus propositus desinet vel in 1, vel in 3, vel in 7 vel in 9; casum quo in 5 desinit hic omitto, quia diuisor 5 tum est manifestus, et indicat numerum non esse primum. Deinde numeri quadrati incipiendo a maximis ipso numero proposito minoribus successiue ab eo subtrahantur, vt pateat, vtrum vnquam numerus quadratus restet, quoties enim hoc euenit, toties resolutio in duo quadrata succedit.

At cum numeri quadrati in nullum horum numerorum 2, 3, 7, 8, desinere queant, subtractio eorum numerorum quadratorum, qui residua dant in hos numeros desinentia omitti poterit. Hinc tantum opus est vt a numero proposito ea quadrata subtrahantur, quae residua in 0, 1, 4, 5, 6, 9, desinentia praebent; nempe

Si numerus propositus desinat in	Quadrata subtrahenda desinent in	Et horum quadratorum radices desinent in.
1	0, 1, 5, 6,	0, 1, 4, 5, 6, 9
3	4, 9	2, 3, 7, 8
7	1, 6	1, 4, 6, 9
9	0, 4, 5, 9	0, 2, 3, 5, 7, 8

Pro quolibet igitur numero proposito $4n + 1 = N$ tot operationes seorsim instituantur, quot radicum idoneae sunt terminationes. Sit igitur pp maximum quadratum huius indolis, quod a numero propoſito N ſubtrahi debet; ac tum ſucceſſiue ſubtrahantur quadrata $(p-10)^2$, $(p-20)^2$, $(p-30)^2$, $(p-40)^2$, etc. Verum reſidua hinc emergentia expedite per continuam additionem inueniri poterunt; Hoc modo

$$\begin{array}{lr}
\text{Numerus propoſitus} & N \\
\text{a quo ſubtrahatur} & pp \\
\hline
 & N-pp \\
\text{Addatur} \;\ldots & 20p-100 \\
\hline
 & N-(p-10)^2 \\
\text{Addatur} \;\ldots & 20p-300 \\
\hline
 & N-(p-20)^2 \\
\text{Addatur} \;\ldots & 20p-500 \\
\hline
 & N-(p-30)^2
\end{array}$$

Numeri igitur ſucceſſiue addendi ſunt: $20p-100$, $20p-300$, $20p-500$, $20p-700$, etc. qui decreſcunt in ratione Arithmetica per differ. $=200$. Huiusmodi operatio pro ſingulis numeris p, quorum quadrata numero propoſito proxime ſunt minora, et qui deſinunt in aliquem figurarum ſupra indicatarum, inſtituatur, neque vlterius continuetur, quam donec ad ſemiſſem numeri propoſiti N perueniatur. Si enim numerus N fuerit ſumma duorum quadratorum, alterum certe ſemiſſe ipſius minus ſit neceſſe eſt. Quo obſeruato, quot hac operatione prodibunt quadrata, tot modis numerus propoſitus in duo quadrata erit reſolubilis. Hanc autem operationem non admodum eſſe moleſtam, omnibusque aliis methodis numeros primos explorandi longe anteferendam, ſequentia exempla declarabunt.

Exem-

EXEMPLVM 1.

§. 45. *Explorare vtrum hic numerus 82421 primus sit nec ne?*

Operatio per sex columnas sequentes instituetur.

p 82421	p 82421	p 82421	p 82421	p 82421	p 82421
286. 81796	285. 81225	284. 80656	281. 78961	280. 78400	279. 77841
□ 625	1196	1765	3460	4021	4580
5620	5600	5580	5520	5500	5480
6245	6796	7345	8980	9521	10060
[illegible]	5400	5380	5320	5300	5280
11665	12196	12725	14300	14821	15340
5220	5200	5180	5120	5100	5080
16885	17396	17905	19420	15921	20420
5020	5000	4980	4920	4900	4880
21905	22396	22885	24340	2482	25300
4820	4300	4780	4720	4700	4680
26725	27196	27665	29060	29521	29980
4620	4600	4580	4520	4500	4480
31345	31796	32245	33580	34021	34460
4420	4400	4380	4320	4300	[illegible]
35765	36196	36625	37900	38321	[illegible]
4220	4200	4180	4120	4100	4080
39985	40396	40805	42020	42421	42820

Cum igitur hic vnicum occurrat quadratum 625, ideoque numerus propositus 82421 vnico modo sit in duo quadrata resolubilis nempe $= 25^2 + 286^2$, is erit primus.

SCHOLION.

§. 46. In hoc computo quatuor columnae, vbi numeri residui desinunt vel in 5 vel in 0, notabiliter contrahi possunt, omittendis omnibus iis, qui non desinunt vel in 25 vel in 00. Quare in columnis, in quibus residua desinunt vel in 5 vel in 0, subtrahatur primo proximum quadratum, quod residuum praebet vel in 25 vel in 00 desinens, hocque quadratum dicatur pp, vt residuum sit $= N - pp$: tum quadrata, vnde residua simili modo desinentia oriuntur, erunt $(p-50)^2$, $(p-100)^2$, $(p-150)^2$ etc. ideoque haec residua obtinebuntur si ad $N-pp$ continuo addantur hi numeri $100p-2500$; $100p-17500$; $100p-125000$ qui decrescunt arithmetice secundum differentiam constantem 5000; vnde hae columnae mox ad finem perducentur, dum eas non vltra semissem numeri propositi continuari opus est. Hoc igitur compendium locum habebit in numeris vel in 1 vel in 9 desinentibus, qui propterea, etiamsi sex columnas requirant, dum pro reliquis quatuor sufficiunt, facilius expedientur.

EXEMPLVM 2.

§. 47. *Explorare vtrum bic numerus* 100981 *primus sit nec?*

p	100981	p	100981	p	100981	p	100981
316.	99856	315.	99225	309.	95481	310.	96100
	1125		1756		5500		4881
	29100		6200		28400		6100
	30225		7956		33900		10981
	24100		6000		23400		5900
	* 54325		13956		* 57300		16881
p	100981		5800		100981		5700
284	80656		19756	291.	84681		22581
	20326		5600		16300		5500
	25900		25356		26600		28081
215^2	$= 46225$		5400		42900		5300
			30756		21600		33381
			5200		* 64500		5100
			35956				38481
			5000				4900
			40956				43381
			4800				4700
			45756				48081
			4600				
			50356				

Cum

Cum ergo vnicum occurrat quadratum $46225 = 215^2$ vnde fit $100981 = 215^2 + 234^2$, erit hic numerus primus.

EXEMPLVM 3.

§. 48. *Explorare vtrum hic numerus* 1000009 *fit primus nec ne?*

p	
	1000009
1000	1000000
1^2	9
	19900
	19909
	19700
	39609
	19500
	59109
	19300
	78409
	19100
	97509
	18900
	116409
	18700
	135109
	18500
	153609
	18300
	171909
	18100
	190009
	17900
	207909
	17700
	225609
	17500
	243109
	17300
	260409
	17100
	277509
	16900
	294409
	16700
	311109
	16500
	327609
	16300
	343909
	16100
*	
*	
	360009
	15900
	375909
	15700
	391609
	15500
	407109
	15300
	422409
	15100
	437509
	14900
	452409
	14700
	467109
	14500
	481609
	14300
	495909

p	
	1000009
978..	956484
	43525
	95300
	138825
	90300
	229125
	85300
	314425
	80300
	394725
	75300
	470025

p	
	1000009
972	944784
235^2	55225
	94700
	149925
	89700
	239625
	84700
	324325
	79700
	404025
	74700
	478725

p	
	1000009
997..	994009
	6000
	97200
	103200
	92200
	195400
	87200
	282600
	82200
	364800
	77200
	442000

	1000009
953..	908209
	91800
	92800
	184600
	87800
	272400
	82800
	355200
	77800
	433000

	1000009
995.	990025
	9984
	19800
	29784
	19600
	49384
	19400
	69784
	19200
	88984
	19000
	107984
	18800
	126784
	18600
	145384
	18400
	163784
	18200
	181984
	18000
	199984
	17800
	217784
	17600
	235384
	17400
	252784
	17200
	269984
	17000
	286984
	16800
	303784
	16600
	320384
	16400
	336784
	16200
	352984
	16000
*	
*	
	368984
	15800
	384784
	15600
	400384
	15400
	415784
	15200
	430984
	15000
	445984
	14800
	460784
	14600
	475384
	14400
	489784

Hic

Hic ergo numerus 1000009 duplici modo est in duo quadrata resolubilis quippe $= 1000^2 + 3^2 = 235^2 + 972^2$, vnde is non erit primus: factores vero eius reperientur ex hac formula $\frac{1000 \pm 972}{235 \pm 3}$ ad minimos terminos reducta, vnde oritur: $\frac{1000+972}{235+3} = \frac{1972}{238} \overset{2}{\Big|} \frac{986}{119} \overset{17}{\Big|} \frac{58}{7}$ ergo factor $= 3413$

$\frac{1000+972}{235-3} = \frac{1972}{232} \overset{4}{\Big|} \frac{493}{58} \overset{29}{\Big|} \frac{17}{2}$ ergo factor $= 293$

qui factores facilius inuenientur ex formula $\frac{1000 - 972}{235 \pm 3}$ $\frac{28}{238} = \frac{14}{119} = \frac{2}{17}$ et $\frac{28}{232} = \frac{7}{58}$.

Nouimus ergo esse $1000009 = 293 \cdot 3413$, qui factores nulla alia methodo tam facile reperti fuissent.

EXEMPLVM 4.

§ 49. *Explorare vtrum hic numerus 233033 primus sit nec ne?*

$482^2 =$ 233033 / 232324	$477^2 =$ 233033 / 227529	$473^2 =$ 233033 / 223729	$478^2 =$ 233033 / 228484
709 / 9540	5504 / 9440	9304 / 9360	4549 / 9460
10249 / 9340	14944 / 9240	18664 / 9160	14009 / 9260
19589 / 9140	24184 / 9040	27824 / 8960	23269 / 9060
28729 / 8940	33224 / 8840	36784 / 8760	32329 / 8860
37669 / 8740	42064 / 8640	45544 / 8560	41189 / 8660
46409 / 8540	50704 / 8440	54104 / 8360	49849 / 8460
54949 / 8340	59144 / 8240	62464 / 8160	58309 / 8260
63289 / 8140	67384 / 8040	70624 / 7960	66569 / 8060
71429 / 7940	75424 / 7840	78584 / 7760	74629 / 7860
79369 / 7740	83264 / 7640	86344 / 7560	82489 / 7660
87109 / 7540	90904 / 7440	93904 / 7360	90149 / 7460
94649 / 7340	98344 / 7240	101264 / 7160	97609 / 7260
101989 / 7140	105584 / 7040	108424 / 6960	104869 / 7060
109129 / 6940	112624 / 6840	115384 / 6760	111929 / 6860
116069	* 119464	* 122144	* 118789

Quia

Quia ergo hic numerus, etsi est formae $4n + 1$, non est summa duorum quadratorum, vi *Prop. V.* colligimus eum non esse numerum primum. Factores quidem eius hinc assignare non licet, interim tamen concludimus eum saltem duos habere factores formae $4m - 1$: qui, inuestigatione instituta, reperientur 467. 499.

E X E M P L V M 5.

§. 50. *Explorare vtrum hic numerus* 262657 *primus sit nec ne?*

262657	262657	262657	262657
$511^2 =$ 261121	$509^2 =$ 259081	$506^2 =$ 256036	$504^2 =$ 254016
1536	3576	6621	8641
10120	10080	10020	9980
11656	13656	$129^2 =$ 16641	18621
9920	9880	9820	9780
21576	23536	26461	28401
9720	9680	9620	9580
31296	33216	36081	37981
9520	9480	9420	9380
40816	42696	45501	47361
9320	9280	9220	9180
50136	51976	54721	56541
9120	9080	9020	8980
59256	61056	63741	65521
8920	8880	8820	8780
68176	69936	72561	74301
8720	8680	8620	8580
76896	78616	81181	82881
8520	8480	8420	8380
85416	87096	89601	91261
8320	8280	8220	8180
93736	95376	97821	99441
8120	8080	8020	7980
101856	103456	105841	107421
7920	7880	7820	7780
109776	111336	113661	115201
7720	7680	7620	7580
117496	119016	121281	122781
7520	7480	7420	7380
125016	126496	128701	130161
7320	7280	7220	7180
* 132336	* 133776	* 135921	* 137341

Cum igitur hic vnicum quadratum occurrat $16641 = 129^2$ ita vt sit vnico modo $262657 = 129^2 + 496^2$, hique

numeri

numeri 129 et 496 sint inter se primi, certum est numerum 262657 esse primum.

EXEMPLVM 6.

§. 51. *Explorare vtrum hic numerus* 32129 *sit primus nec ne?*

32129	32129	32129	32129
$152^2 = 23104$	$177^2 = 31329$	$175^2 = 30625$	$170^2 = 28900$
$95^2 = 9025$	800	1504	3229
12700	15200	3400	3300
* 21725	16000	4904	6529
		3200	3100
32129	32129	8104	9629
$148^2 = 21904$	$173^2 = 29929$	3000	2900
10225	2200	11104	12529
12300	14800	2800	2700
* 22525	* 17000	13904	15229
		2600	2500
		* 16504	* 17729

Hic igitur numerus quoque vnico modo est in duo quadrata resolubilis $= 95^2 + 152^2$, sed quia hi numeri 95 et 152 non sunt primi inter se, sed communem diuisorem habent 19, numerus propositus non erit primus, sed factorem habet $19^2 = 361$, estque $32129 = 19^2 . 89$.

SCHOLION.

§. 52. Quanquam haec methodus explorandi numeros vtrum sint primi nec ne? tantum ad numeros in hac forma $4n + 1$ contentos extenditur, tamen saepe numero in diiudicandis numeris magnum subsidium afferre potest. Quantum autem aliis regulis hoc idem praestandi antecellat, quilibet, qui periculum huius rei facere velit, facile experietur. Qui enim numerum millione non minorem via consueta examinare voluerit, eius diuisionem per omnes numeros primos ad millenarium vsque tentare debet, quod opus intra plures horas non absoluet: dum ope huius regulae ipsi vix semihora opus erit.

DE CON-