SPECIMEN
DE VSV OBSERVATIONVM
IN MATHESI PURA.

Auctore

L. EVLERO.

Inter tot insignes numerorum proprietates, quae adhuc sunt inuentae ac demonstratae, nullum est dubium, quin pleraeque primum ab inuentoribus tantum sunt obseruatae et in multiplici numerorum tractatione animaduersae, antequam de iis demonstrandis cogitauerint. Ita de eo numerorum primorum ordine, qui vnitate superant multiplum quaternarii, cuiusmodi sunt 5, 13, 17, 29, 37, 41, etc. ante sine dubio est obseruatum, eorum singulos in duo quadrata secari posse, quam in eo elaboratum, vt huius obseruationis veritas per solidam demonstrationem euinceretur. Quod deinde quilibet numerus in quatuor vel pauciora quadrata distribui possit, Diophanto iam notum fuisse videtur, nemo autem ante Fermatium est professus, se huius veritatis demonstrationem habere, quam autem nusquam publice edidit, ita vt mea demonstratio, quam ante aliquod tempus concinnaui, pro prima, quae quidem publice fuerit proposita, sit habenda. Interim tamen fateri cogor, demonstrationem Fermatianam, etiamsi mihi nihil omnino de principiis, quibus innitebatur, suspicari licuerit, mea multo fuisse perfectiorem, ac longe latius patuisse.

Asseuerat enim Fermatius, se ex eodem fonte aliorum quoque Theorematum demonstrationes hausisse, cuius generis sunt, quod omnis numerus integer sit summa trium pauciorumue numerorum trigonalium; item quod omnis numerus integer sit summa quinque vel pauciorum numerorum pentagonalium; item sex pauciorumue numerorum hexagonalium, et ita porro de reliquis numeris polygonalibus in infinitum. Ego vero etiamsi resolutionem cuiusque numeri in quatuor pauciorue quadrata demonstraui, tamen omnem adhuc operam in istis reliquis theorematibus demonstrandis inutiliter consumsi, neque vllo modo etiam nunc saltem resolutionem in tres paucioresue trigonales ostendere potui, etiamsi ea simplicior videatur, quam resolutio in quatuor pauciorue quadrata. Verum et has eximias numerorum proprietates Fermatius multo ante per inductionem conclusisse est putandus, quam eas demonstrare didicerit. Ex quibus merito colligimus, in numerorum indole scrutanda obseruationi et inductioni, cui omnes has elegantissimas proprietates acceptas referre debemus, plurimum esse tribuendum; ideoque ne nunc quidem ab hoc negotio vlterius prosequendo esse desistendum. Hoc enim modo pertingimus ad huiusmodi proprietatum cognitionem, quae alias nobis perpetuo ignotae mansissent; ac tum demum occasionem nanciscimur ad inuestigationem demonstrationum vires nostras intendendi; veritates namque pleraeque huius generis ita sunt comparatae, vt prius agnosci debeant, quam demonstrari possint. Quamuis autem huiusmodi proprietas per assiduam obseruationem fuerit animaduersa, quae per se menti non

parum

parum eſt iucunda: tamen niſi demonſtratio ſolida acceſſerit, de eius veritate non ſatis certi eſſe poſſumus; exempla enim non deſunt, quibus ſola inductio in errorem praecipitauerit. Tum vero ipſa demonſtratio non ſolum omnia dubia tollit, ſed etiam naturae numerorum penetralia non mediocriter recludit, noſtramque numerorum cognitionem continuo magis promouet, a cuius certe doctrinae perfectione adhuc longiſſime ſumus remoti. Verum ſi cui haec forte non magni momenti eſſe videantur, quod vix vnquam vllum in Matheſi applicata vſum habitura putentur, vſus quem inde in ratiocinando adipiſcimur, certe non eſt contemnendus. Sunt enim plerumque huius generis veritates ita reconditae, vt earum demonſtrationes tam incredibilem circumſpectionem, quam eximiam ingenii vim requirant. Quare cum vulgo ad ratiocinii facultatem comparandam demonſtrationes geometricae commendari ſoleant, quippe quae regularum rationandi vſum maxime contineant, neſcio an non ad hunc ſcopum demonſtrationes arithmeticae multo magis ſint accommodatae: in his enim multo maiori cura eſt cauendum, ne a praeſcriptis Logicorum regulis aberremus, quoniam plerumque nimis eſt difficile, in errorem non prolabi. Deinde vero huius generis demonſtrationes arithmeticae, multo maiorem ſollertiam et ſagacitatem ingenii poſtulant, quam geometricae: vnde qui in his fuerit exercitatus, longe facilius errorem in ratiocinando vſu edoctus euitabit, ſibique promtum ratiocinii vſum multo certius comparabit. Atque, ob haec tam inſignia commoda, perluſtrationes naturae numerorum minime relinquendae

videntur, in quibus ne inutiliter verſemur, ab obſeruationibus erit exordiendum, hincque ad demonſtrationem proprietatum obſeruatarum progrediendum. Huiusmodi operationem iam ante aliquot annos confeci in contemplatione diuiſorum cuiusque numeri, qui eſt ſumma duorum quadratorum, nunc igitur, vt viam ad alias numerorum proprietates cognoſcendas ſternam, contemplaturus ſum numeros, qui ex quadrato et duplo quadrati ſunt compoſiti, quales in hac forma generali $2aa+bb$ ſunt contenti, atque in diuiſores horum numerorum ſum inquiſiturus. At hic quidem ſtatim notari conuenit, radices horum duorum quadratorum numeros inter ſe primos eſſe oportere, alioquin enim quilibet numerus poſſet eſſe diuiſor, quadratum ſcilicet numeri, qui foret radicum communis diuiſor: quam ob rem numeros a et b, ex quibus forma $2aa+bb$ componitur, inter ſe primos ſtatuam.

CONSIDERATIO CIRCA NVMEROS in hac forma $2aa+bb$ contentos.

Exponantur primo numeri in forma $2+bb$ contenti, tum numeri huius formae $8+bb$, excluſis numeris paribus pro b ſubſtituendis: tertio numeri formae $18+bb$, ſumendo pro b numeros per 3 non diuiſibiles: quarto numeros formae $32+bb$, ſumendo pro b numeros per 2 non diuiſibiles, et ita porro. Sicque obtinebuntur ſequentes numerorum progreſſiones:

$2+bb$) 5, 6, 11, 18, 27, 38, 51, 66, 83, 102, 123, 146, 171, 198, 227, 258, 291, 326, 363, 402, 443, 486.

$8+bb$)

$8+bb$) 9, 17, 33, 57, 89, 129, 177, 233, 297, 349, 449.
$18+bb$) 19, 22, 34, 43, 67, 82, 118, 139, 187, 214, 274, 307, 379, 418.
$32+bb$) 33, 41, 57, 81, 113, 153, 201, 257, 321, 393, 473.
$50+bb$) 51, 54, 59, 66, 86, 99, 114, 131, 171, 194, 219, 246, 306, 339, 374, 411, 491.
$72+bb$) 73, 97, 121, 193, 241, 361, 433.
$98+bb$) 99, 102, 107, 114, 123, 134, 162, 179, 198, 219, 242, 267, 323, 354, 387, 422, 459, 498.
$128+bb$) 129, 137, 153, 177, 209, 249, 297, 353, 417, 489.
$162+bb$) 162, 166, 178, 187, 211, 226, 262, 283, 331, 358, 418, 451.
$200+bb$) 201, 209, 249, 281, 321, 369, 489.
$242+bb$) 243, 246, 251, 258, 267, 278, 291, 306, 323, 342, 386, 411, 438, 467, 498.
$288+bb$) 289, 313, 337, 409, 457.
$338+bb$) 339, 342, 347, 354, 363, 374, 387, 402, 419, 438, 459, 482.
$392+bb$) 393, 401, 417, 473.
$450+bb$) 451, 454, 466, 499.

Obſeruatio I.

Excerpamus hinc numeros primos, vt nanciſcamur omnes numeros primos formae $2aa+bb$, qui quidem 500 non ſuperent, quippe ad quem terminum omnes progreſſiones praecedentes produximus, atque iſti numeri primi reperientur eſſe:

3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97, 107, 113, 131, 137, 139, 163, 179, 193, 211, 227, 233, 241, 251, 257, 280, 283, 307, 313, 331, 337, 347, 353, 379, 401, 409, 419, 433, 443, 449, 457, 467, 491, 499.

De his ergo obseruo, singulos nonnisi semel in serie numerorum formae $2aa+bb$ occurrere: *ita vt numerus primus, qui fuerit aggregatum ex quadrato et duplo quadrato, sit vnico modo huiusmodi aggregatum.*

Obseruatio 2.

Si ex numeris expositis excerpantur ii, qui sunt producta ex binario et numero primo, illi in ordinem digesti erunt:

6, 22, 34, 38, 82, 86, 118, 134, 146, 166, 178, 194, 214, 226, 262, 274, 278, 326, 358, 386, 422, 454, 466, 482.

vbi alii numeri non occurrunt, nisi ipsi numeri primi formae $2aa+bb$ duplicati, ac singuli hi quidem numeri semel tantum reperiuntur.

Qui ergo numerus primus in forma $2aa+bb$ fuerit contentus, eius quoque duplum erit numerus formae $2aa+bb$, idque vnico modo.

Ceterum cum a et b sint numeri inter se primi, ideoque alter eorum certo impar, manifestum est, nullos dari in forma $2aa+bb$ numeros per 4 diuisibiles.

Obser-

Obſeruatio 3.

Cum in numeris expoſitis alii ſint impares, alii pares, et quidem impariter pares, obſeruo porro:

Si quis numerus impar inter illos numeros reperiatur, tum quoque eius duplum certo occurrere; ac viciſſim quicunque numerus par in illis numeris occurrit, eius quoque ſemiſſis ibidem certo reperietur.

Obſeruatio 4.

Quodſi iam reliquos numeros non primos ſpectemus, ſingulosque in ſuos factores primos reſoluemus, vnicuique autem in parentheſi adſcribamus, quod vicibus occurrat, ſequentes nanciſcemur:

$3^2(1)$; $3^3(1)$; $3.11(2)$; $3.17(2)$; $3.19(2)$; $3^4(1)$; $3^2.11(2)$; $11^2(1)$; $3.41(2)$; $3.43(2)$; $3^2.17(2)$; $3^2.19(2)$; $3,59(2)$; $11.17(2)$; $3.67(2)$; $11,19(2)$; $3,73(2)$; $3^5(1)$; $3,83(2)$; $3,89(2)$; $17^2(1)$; $3.97(2)$; $3^3.11(2)$; $3,107(2)$; $17.19(2)$; $3\ 113(2)$; $19^2(1)$; $3,11^2(2)$; $3^2,41(2)$; $3^2,43(2)$; $3,131(2)$; $3,137(2)$; $3.139(2)$; $11.41(2)$; $3^3,17(2)$; $11.43(2)$; $3.163(2)$.

Hic iam obſeruo omnia producta ex numeris primis formae $2aa+bb$ per quamcunque combinationem nata occurrere: *ita vt productum ex quotcunque numeris formae* $2aa+bb$ *ſemper ſit numerus in quadratum et duplum quadratum reſolubilis*: ac plus quidem vno modo, ſi ex diuerſis factoribus fuerit conflatus.

Obſer-

Obſeruatio 5.

Imprimis autem hic animaduerto, in his numeris compoſitis nullos alios factores primos occurrere, niſi qui ipſi ſint formae $2aa+bb$; vnde colligo per inductionem:

Omnes numeros formae $2aa+bb$, *ſi quidem* a *et* b *ſint numeri inter ſe primi, nullos alios diuiſores admittere primos, niſi qui ipſi ſint huius formae* $2aa+bb$.

Binarium quidem vidimus inter diuiſores occurrere poſſe, verum cum $2aa+bb$ caſu $b=0$ et $a=1$ binarium praebeat, etiam ipſum binarium in forma $2aa+bb$ complecti licet.

Obſeruatio 6.

Cum ergo omnis numerus formae $2aa+bb$, exiſtentibus a et b primis inter ſe, alios diuiſores primos non admittat, niſi qui in ſerie numerorum in obſeruatione prima exhibitorum contineantur, ſi ipſis quidem binarius adiungatur: circa iſtos numeros primos obſeruo, intra illos nullos numeros ſiue huius formae $8n-1$, ſiue huius $8n-3$ reperiri.

De numeris ergo primis formae $8n-1$ et $8n-3$ *affirmare licet, eos non ſolum non eſſe numeros formae* $2aa+bb$, *ſed etiam ne diuiſores quidem eſſe poſſe vllius numeri formae* $2aa+bb$, *ſiquidem* a *et* b *ſint primi inter ſe.*

Obſeruatio 7.

Numeris ergo primis huius geminae formae $8n-1$ et $8n-3$ excluſis, praeter binarium nulli alii relin-

relinquuntur numeri primi, qui sint diuisores numerorum formae $2aa+bb$, nisi qui in alterutra harum formarum $8n+1$, vel $8n+3$, contineantur; quos duplicis generis numeros primos conspectui exposuisse iuuabit:

$(8n+1)$: 17, 41, 73, 89, 97, 113, 137, 193, 233, 241, 257, 281, 313, 337, 353, 401, 409, 433, 449, 457.

$(8n+3)$: 3, 11, 19, 43, 59, 67, 83, 107, 131, 139, 163, 179, 211, 227, 251, 283, 307, 331, 347, 379, 419, 443, 467, 491, 499.

atque obseruo, hos numeros primos omnes inter numeros primos formae $2aa+bb$ ita occurrere, vt alii praeterea ibi non reperiantur.

Hinc ergo numeri huius formae $2aa+bb$, *dummodo* a *et* b *sint inter se primi, praeter binarium nullos alios habent diuisores primos, nisi qui sint vel huius formae* $8n+1$, *vel huius* $8n+3$.

Cum autem omnes numeri primi in his quatuor formis $8n+1$ et $8n+3$ contineantur, haec obseruatio cum praecedente conuenit.

Obseruatio 8.

At, quod notatu maxime est dignum, obseruo: *Omnem numerum primum tam huius formae* $4n+1$, *quam huius* $8n+3$, *semper esse aggregatum ex quadrato et duplo quadrato: siue inter numeros primos formae* $2aa+bb$ *omnes plane numeros, siue huius formae* $8n+1$, *siue huius* $8n+3$ *occurrere, ac praeterea nullos alios.*

Nullus ergo assignari poterit numerus primus in harum formularum $8n+1$ et $8n+3$ alterutra contentus, qui non sit summa quadrati et dupli quadrati, et hoc quidem vnico modo, si obseruatio prima huc trahatur.

Nota.

Proprietatum, quas hic circa numeros formae $2aa+bb$ eorumque diuisores obseruauimus, aliae ita sunt comparatae, vt earum veritas facile ostendi possit, aliae autem maiorem demonstrationis apparatum requirunt, aliae vero denique profundissimae indaginis sunt indicandae, cum summa sollertia ad eas demonstrandas sit opus. Ad primum genus referendae sunt obseruationes prima, secunda, tertia, quarta et pars prior sextae; ad genus secundum autem pertinent obseruationes quinta, pars posterior sextae, et septima, quae eo redit. Profundissimae autem indaginis est obseruatio octaua. Proprietates autem istae similes sunt iis, quas circa summas duorum quadratorum proposui; quarum veritatem cum feliciter eruerim, operam dabo, vt etiam has proprietates obseruatas simili modo demonstrationibus confirmem. Incipiam ergo ab obseruationibus facillimis.

Theorema. I.

I. Si numerus N fuerit numerus formae $2aa+bb$, tum quoque eius duplum 2N erit numerus eiusdem formae.

Demon-

Demonstratio.

Sit enim $N = 2mm + nn$, erit $2N = 4mm + 2nn$, ponatur $2m = k$, fietque $2N = kk + 2nn$, sicque $2N$ erit quoque numerus formae $2aa + bb$. Q. E. D.

Coroll. 1.

2. Ac si N fuerit pluribus modis numerus formae $2aa + bb$, totidem quoque modis eius duplum $2N$ erit numerus formae $2aa + bb$.

Coroll. 2.

3. Constat ergo veritas obseruationis secundae, simulque ratio perspicitur, cur numerorum, qui inter numeros formae $2aa + bb$ supra expositos bis occurrunt, eorum quoque dupla ibidem bis reperiantur.

Theorema 2.

4. Si numerus par $2N$ fuerit numerus formae $2aa + bb$, tum quoque eius semissis N erit numerus eiusdem formae.

Demonstratio.

Posito $2N = 2mm + nn$, quo $2mm + nn$ sit numerus par, quoniam pars $2mm$ iam est par, necesse est, vt altera pars nn sit quoque numerus par, ideoque et eius radix n. Ponatur ergo $n = 2k$, fietque $2N = 2mm + 4kk$, vnde per 2 diuidendo oritur $N = mm + 2kk$, ita vt quoque semissis N sit in forma $2aa + bb$ contentus. Q. E. D.

Coroll. 1.

5. Hinc etiam euidens est, si numerus propositus par 2N fuerit pluribus modis numerus formae $2aa+bb$, totidem quoque modis eius semissem N fore numerum eiusdem formae.

Coroll. 2.

6. Si ergo numerus N fuerit vnico modo numerus formae $2aa+bb$; tum etiam eius duplum 2N vnico modo erit numerus formae $2aa+bb$; si enim pluribus modis esset huius formae, totidem quoque modis eius semissis N foret eiusdem formae contra hypothesin.

Coroll. 3.

7. Hinc autem porro duplicando numeri 4N, 8N, 16N etc. omnes vnico tantum modo in forma $2aa+bb$ continebuntur, siquidem numerus simplex N vnico modo in ista forma reperiatur.

Coroll. 4.

8. Quod vero hic de vnico modo resolutionis in formam $2aa+bb$ est dictum, patet quoque ad duos pluresue modos. Ex qualibet enim resolutione numeri N in formam $2aa+bb$, sponte nascitur resolutio numeri, siue dupli, siue dimidii, sicque obseruationem tertiam demonstratam dedimus.

Theo-

Theorema 3.

9. Si habeantur duo numeri M et N formae $2aa+bb$, erit quoque eorum productum MN numerus eiusdem formae.

Demonstratio.

Sit enim $M=2aa+bb$, et $N=2cc+dd$, erit eorum productum

$$MN=4aacc+2aadd+2ccbb+bbdd;$$

addatur $0=4acbd-4acbd$, et habebitur

$$MN=4aacc+4acbd+bbdd+2aadd-4acbd+2ccbb$$

quae expressio manifesto est aggregatum ex quadrato et duplo quadrato, scilicet:

$$MN=(2ac+bd)^2+2(ad-cb)^2$$

Vel quod eodem redit, si terminos $+4acbd$ et $-4acbd$ permutemus, vt sit

$$MN=4aacc-4acbd+bbdd+2aadd+4acbd+2ccbb$$

habebimus quoque alio modo

$$MN=(2ac-bd)^2+2(ad+cb)^2$$

Quare si vterque numerus M et N fuerit formae $2aa+bb$, erit quoque productum numerus eiusdem formae. Q. E. D.

Coroll. 1.

10. Ob geminas formulas inuentas productum MN erit duplici modo numerus formae $2aa+bb$. Si enim sit

$$M=2aa+bb \text{ et } N=2cc+dd$$

ac ponatur productum $MN = 2pp + qq$, erit

vel $p = ad - cb$ et $q = 2ac + bd$

vel $p = ad + cb$ et $q = 2ac - bd$.

Coroll. 2.

11. Si fuerit vel $ad - cb$, vel $2ac - bd$ numerus negatiuus, pro p et q eorum valorés affirmatiui assumi poterunt; ex formulis enim quadratis perinde elicere licuisset priori casu $p = cb - ad$, posteriori vero $q = bd - 2ac$. Numeri igitur negatiui hoc modo pro radicibus quadratorum oriundi calculum nihil turbant.

Coroll. 3.

12. Productum ergo duorum numerorum formae $2aa + bb$ duplici modo in eandem formulam resolui poterit, nisi forte vtraque resolutio ad eandem recidat, quod autem non euenit, nisi fuerit vel $cb = 0$ et $bd = 0$, vel $ac = 0$, hoc est $b = 0$, vel $a = 0$, vel $c = 0$, vel etiam $d = 0$, alterque propterea numerorum propositorum, vel quadratus, vel duplum quadrati.

Coroll. 4.

13. Si ergo ambo numeri fuerint primi, eorum productum semper est duplici modo resolubile in formam $2aa + bb$, nisi alter fuerit $= 1$, vel $= 2$. Cum enim tantum excipiantur casus, quibus alter est quadratum, vel duplum quadratum, vterque autem pona-

tur

tur primus, excipiuntur tantum casus, quibus alter est vel 1, vel 2.

Coroll. 5.

14. Si ambo numeri M et N fuerint aequales, seu $N = M$, vt sit $c = a$ et $d = b$, erit quidem duplici modo quadratum $MM = 2pp + qq$; scilicet vel $p = 0$ et $q = 2aa + bb$, vel $p = 2ab$ et $q = 2aa - bb$. Sed prior resolutio $MM = 2.0^2 + (2aa + bb)^2$, minus ad scopum pertinere est censenda, quia alterum quadratum est euanescens. Sin autem esset, vel $a = 0$, vel $b = 0$, vtraque resolutio adeo ad vnum rediret.

Coroll. 6.

15. Patet hinc etiam productum ex tribus numeris L, M, N formae $2aa + bb$ quadruplici modo in formam eandem resolui posse. Sit enim:

$$L = 2aa + bb;\ M = 2cc + dd;\ N = 2ee + ff$$

ac sit primo $LM = 2pp + qq$, erit vti vidimus:

vel $p = ad + cb$ et $q = 2ac + bd$

vel $p = ad + cb$ et $q = 2ac - bd$

Tum ergo, si ponatur productum $LMN = 2xx + yy$, erit quoque duplici modo

vel $x = pf - eq$ et $y = 2ep + fq$

vel $x = pf + eq$ et $y = 2ep - fq$

Hinc ergo, pro p et q valoribus inuentis substituendis, reperietur

I. vel

I. vel $x = 2ace + bde + bcf - adf$ et $y = 2ade + 2acf - 2bce + bdf$
II. vel $x = 2ace - bde - bcf - adf$ et $y = 2ade + 2acf + 2bce - bdf$
III. vel $x = 2ace + bde - bcf + adf$ et $y = 2ade - 2acf - 2bce - bdf$
VI. vel $x = 2ace - bde + bcf + adf$ et $y = 2ade - 2acf + 2bce + bdf$

Coroll. 7.

16. Simili modo colligitur, productum ex quatuor numeris formae $2aa + bb$ octo diuersis modis in formam eandem resolui posse; casus tamen sunt excipiendi, quibus inter numeros propositos reperiuntur, vel aequales, vel simplicia quadrata, vel quadrata dupla: his enim casibus vidimus resolutiones, quae in genere sunt diuersae, conuenire.

Scholion.

17. Quod autem ad istas resolutiones attinet, earum vis perfecte intelligi nequit, nisi demonstrauerimus, numeros primos plus vno modo in hac forma $2aa + bb$ non contineri. Si enim numeri primi plurimis modis essent resolubiles, de numeris compositis nihil certi definiri posset, nisi quod adhuc pluribus modis huiusmodi resolutiones admittant. Cum igitur prima obseruatio nos docuerit, numeros primos, qui quidem in ordine numerorum formae $2aa + bb$ continentur, nonnisi semel ibidem occurrere, hanc ipsam veritatem demonstrare aggrediar.

Theorema. 4.

18. Qui numerus duplici modo in formam $2aa + bb$ resolui potest, is non est primus.

Demon-

Demonstratio.

Sit numerus N duplici modo in hanc formam resolubilis, ac ponatur

$$N = 2aa + bb \text{ et } N = 2cc + dd$$

ita vt tam numeri a et c, quam b et d, sint diuersi. Multiplicetur prior aequatio per cc, altera per aa, atque illa ab hac subtracta, relinquet:

$$(aa - cc)N = aadd - bbcc = (ad - bc)(cd + bc)$$

Quod si iam numerus N esset primus, is in alterutro factore $ad - bc$, vel $ad + bc$, contineretur, necesse est. Verum cum addendis nostris formulis sit $2N = 2aa + bb + 2cc + dd$, auferatur vtrinque $2ad + 2bc$, vnde habebitur:

$$2N - 2ad - 2bc = 2aa + bb + 2cc + dd - 2ad - 2bc;$$

siue $2N - 2ad - 2bc = aa + (a-d)^2 + cc + (c-b)^2$. At postremum hoc membrum, vtpote summa quatuor quadratorum, certo est nihilo maius, ita vt sit $2N - 2ad - 2bc > 0$; vnde fit:

$$N > ad + bc.$$

Cum ergo N sit maior, quam $ad + bc$, multoque magis quam $ad - bc$, numerus N in neutro factore $ad - bc$, vel $ad + bc$, tanquam pars continetur. Fieri ergo nequit, vt numerus N, qui duplici modo in formam $2aa + bb$ est resolubilis, sit primus. Q. E. D.

Coroll. 1.

19. Si ergo N fuerit numerus primus, certe plus vno modo in formam $2aa + bb$ non est resolubilis,

bilis, quoniam, si plus vno modo resolui posset, non esset primus, sicque habetur demonstratio obseruationis primae.

Coroll. 2.

20. Quicunque ergo numerus primus vel plane non ad formam $2aa+bb$ reduci potest, vel vnico tantum modo. Cauendum autem, ne hinc vicissim concludatur, omnem numerum, qui vnico tantum modo sit resolubilis, esse primum; huiusmodi enim conclusio regulis ratiocinandi aduersaretur.

Coroll. 3.

21. Si fuerit idem numerus $N=2aa+bb$, itemque $N=2cc+dd$, erit hinc, vt vidimus, $(aa-cc)N=(ad-bc)(ad+bc)$, ideoque:

$$N=\frac{(ad-bc)(ad+bc)}{aa-cc}$$

Numerator ergo huius fractionis non solum per denominatorem erit diuisibilis, sed reductione ad integrum facta, simul factores numeri N innotescent.

Coroll. 4.

22. Hoc ergo casu numerus N non solum non erit primus, sed etiam eius factores hinc facile colligentur. Sic cum numerus 267 bis inter numeros formae $2aa+bb$ occurrat, scilicet:

$$267=2.7^2+13^2 \text{ et } 267=2.11^2+5^2$$

ob $a=7$, $b=13$, $c=11$ et $d=5$, habebimus:

267=

$$267 = \frac{(35-143)(35+143)}{(7-11)(7+11)} = \frac{108.178}{4.18}$$

hincque $267 = \frac{6.178}{4} = 3.89.$

Theorema 5.

23. Si numerus formae $2aa+bb$ fuerit diuisibilis per numerum primum eiusdem formae, tum etiam quotus erit numerus eiusdem formae.

Demonstratio.

Sit numerus propositus $N = 2aa+bb$, eiusque diuisor $P = 2pp+qq$, qui cum sit primus, numeri p et q erunt primi inter se. Denotet Q quotum ex hac diuisione oriundum, ita vt sit

$$Q = \frac{N}{P} = \frac{2aa+bb}{2pp+qq}$$

Cum igitur numerus $N = 2aa+bb$ sit diuisibilis per $P = 2pp+qq$; erit quoque $pp(2aa+bb) = 2aapp + bbpp$ per P diuisibile: at $aaP = 2aapp+aaqq$ etiam manifesto per P est diuisibile, vnde quoque differentia horum numerorum $aaqq-bbpp$, per numerum primum P diuisibilis sit necesse est Quia vero est $aaqq-bbpp = (aq-bp)(aq+bp)$, alter horum duorum factorum $aq \pm bp$, per numerum primum P certo erit diuisibilis. Ponatur ergo

$$aq \pm bp = mP = 2mpp+mqq$$

hincque reperitur:

$$q = \frac{2mpp \mp bp}{q} + mq = \frac{p(2mp \mp b)}{q} + mq.$$

Cum itaque $\frac{p(2mp \mp b)}{q}$ sit numerus integer, numeri autem p et q inter se primi, necesse est, vt $2mp \mp b$ sit per q diuisibile. Ponatur ergo $2mp \mp b = \mp nq$, eritque

$$b = nq \mp 2mp, \text{ et } a = mq \pm np.$$

Hinc autem fit:

$$N = 2aa + bb = \begin{cases} 2mmqq \mp 4mnpq + 2nnpp \\ + nnqq \pm 4mnpq + 4mmpp \end{cases}$$

siue $N = (2mm + nn)(2pp + qq)$

Quodsi ergo hic numerus N diuidatur per numerum primum $P = 2pp + qq$, per quem diuisibilis esse ponebatur, quotus erit $Q = 2mm + nn$, ideoque numerus formae $2aa + bb$. Q. E. D.

Hypothesis.

24 Quoniam in sequentibus frequentissime sermo erit de numeris formae $2aa + bb$, item de numeris primis eiusdem formae: deinde vero etiam de numeris tam primis, quam compositis, qui in hanc formam $2aa + bb$ non sunt resolubiles; ne indolem horum numerorum describendo nimis fiam prolixus, compendii causa sequentibus signis vtamur. Denotent ergo literae initiales alphabethi maiusculae: A, B, C, D, E etc. perpetuo imposterum numeros formae $2aa + bb$, idque in genere, siue sint primi, siue compositi: eaedem vero literae commate notatae: A′, B′, C′, D′, E′ etc. numeros in hac forma non contentos, siue primos, siue compositos. Deinde vero literae initiales alphabethi germanici

manici maiusculae: $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, $\mathfrak{E}$, etc. significent numeros tantum primos formae $2aa+bb$, qui sunt, vt supra vidimus, 3, 11, 17, 19, 41, 43, 59, 67, 73 etc. quibus binarius adiungi potest. Eaedem vero literae commate notatae $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$, $\mathfrak{D}'$, $\mathfrak{E}'$ etc. denotent numeros primos in forma $2aa+bb$ non contentos, qui ergo sunt: 5, 7, 13, 23, 29, 31, 37, 47, 53, 61, 71 etc.

Coroll. 1.

25. Hac ergo notatione recepta in Theoremate antecedente demonstratum est, si numerus A fuerit divisibilis per numerum $\mathfrak{A}$, quotum certo fore numerum B: vel si numerus A vnum factorem habeat $\mathfrak{A}$, alterum factorem fore B, scilicet numerum formae $2aa+bb$. Vel etiam si $\frac{A}{\mathfrak{A}}$ fuerit numerus integer, erit is $=$ B.

Coroll. 2.

26. Si ergo numerus A per numerum quempiam P diuisus producat quotum B', hoc est numerum in forma $2aa+bb$ non contentum, tum diuisor ille P certe non erit $\mathfrak{A}$, seu non erit numerus primus formae $2aa+bb$. Erit ergo vel compositus eiusdem formae, vel plane non istius formae $2aa+bb$.

Coroll. 3.

27 Secundum hunc autem notandi modum in theorematibus praecedentibus demonstrauimus:

In primo scilicet est $2A = B$.
In secundo vero esse $\frac{A}{2} = B$
In tertio esse $AB = C$

In quarto si fuerit $A = B$, seu si idem numerus duplici modo in forma $2aa + bb$ contineatur, tum non esse $A = \mathfrak{A}$.

Theorema 6.

28. Si numerus formae $2aa + bb$ diuisibilis fuerit per numerum, qui ista forma non contineatur, tum quotus neque erit numerus primus formae $2aa + bb$, neque productum ex meris huiusmodi numeris primis conflatum.

Demonstratio.

Demonstrari ergo debet si numerus A diuisibilis fuerit per numerum B', tum quotum neque fore $= \mathfrak{A}$, neque productum huiusmodi $\mathfrak{A}\mathfrak{B}\mathfrak{C}\mathfrak{D}$ etc. Si enim quotus esset $\mathfrak{A}$, seu $\frac{A}{B'} = \mathfrak{A}$, foret $\frac{A}{\mathfrak{A}} = B'$, quod per theorema praecedens fieri nequit. Sin autem quotus esset productum ex quotcunque numeris primis formae $2aa + bb$, scilicet $= \mathfrak{A}\mathfrak{B}\mathfrak{C}\mathfrak{D}$, vt esset $\frac{A}{B'} = \mathfrak{A}\mathfrak{B}\mathfrak{C}\mathfrak{D}$, foret vtique $A = \mathfrak{A}\mathfrak{B}\mathfrak{C}\mathfrak{D}B'$, ideoque $\frac{A}{\mathfrak{A}} = \mathfrak{B}\mathfrak{C}\mathfrak{D}B'$. At est $\frac{A}{\mathfrak{A}} = B$, vnde foret $B = \mathfrak{B}\mathfrak{C}\mathfrak{D}B'$, hincque $\frac{B}{\mathfrak{B}} = \mathfrak{C}\mathfrak{D}B'$: verum simili modo est $\frac{B}{\mathfrak{B}} = C$, ideoque $\frac{C}{\mathfrak{C}} = \mathfrak{D}B'$: at est $\frac{C}{\mathfrak{C}} = D$, et $\frac{D}{\mathfrak{D}} = E$, foret ergo tandem $E = B'$, quod esset absurdum: vnde sequitur, quotum neque fore numerum primum formae $2aa + bb$, neque productum ex meris huiusmodi numeris primis constans. Q. E. D.

Coroll.

Coroll. 1.

29. Cum igitur quotus neque sit numerus primus formae $2aa+bb$, neque ex meris numeris primis huius formae conflatus, factores habebit, vel saltem vnum factorem primum in forma $2aa+bb$ non contentum, seu litera $\mathfrak{A}'$ designandum.

Coroll. 2.

30. Quoniam ergo factores quoti sunt quoque factores diuidendi, perspicuum est, si numerus formae $2aa+bb$ diuisorem habeat B′, seu in forma $2aa+bb$ non contentum, tum eundem numerum insuper alium ad minimum habiturum esse diuisorem primum, in forma $2aa+bb$ non contentum, seu si numerus A′ diuisorem habeat B′, tum certe etiam diuisorem habebit alium $\mathfrak{B}'$.

Coroll. 3.

31. Quod hic in genere de diuisoribus formae A′ ostensum est, valet etiam de diuisoribus formae $\mathfrak{A}'$. Hinc si numerus formae $2aa+bb$ diuisibilis fuerit per numerum primum in eadem forma non contentum, tum etiam quotus est diuisibilis per numerum primum in eadem forma non contentum.

Theorema 7.

32. Si numerus formae $2aa+bb$, quantumuis magnus, diuisorem habuerit numerum P, neque tamen radices a et b ipsae per P sint diuisibiles, tum alius numerus

merus eiusdem formae exhiberi potest minor, quam $\frac{3}{4}$ PP, qui per eundem diuisorem P sit diuisibilis.

Demonstratio.

Posito numero $2aa+bb$ diuisibili per P, quantumuis magnae fuerint radices a et b, eae semper ita exprimi possunt:

$$a = mP \pm c \text{ et } b = nP \pm d$$

vt numeri c et d semissem ipsius P non excedant, neuterque euanescet, cum neque a, neque b, per P sit diuisibile. Sit ergo $c < \frac{1}{2}P$ et $d < \frac{1}{2}P$; atque his valoribus substitutis forma $2aa+bb$ abibit in sequentem:

$$(2mm+nn)PP \pm 4mcP \pm 2ndP + cc + 2dd$$

quae cum sit diuisibilis per P, necesse est, vt quoque eius pars $2cc+dd$ per P sit diuisibilis; quae est et numerus formae $2aa+bb$, et minor quam $\frac{3}{4}PP$. Dato ergo numero formae $2aa+bb$ diuisibili per numerum quemcunque P, semper exhiberi poterit numerus minor, quam $\frac{3}{4}PP$, et eiusdem formae, qui per eundem numerum P futurus sit diuisibilis. Q. E. D.

Coroll. 1.

33. Existente ergo P diuisore cuiuspiam numeri A, dabitur numerus $B < \frac{3}{4}P$ per P diuisibilis, et quotus inde oriundus propterea erit minor quam $\frac{3}{4}P$: qui cum etiam sit diuisor numeri B si P sit diuisor cuiuspiam numeri formae $2aa+bb$, hinc innotescit quoque numerus alius minor quam $\frac{3}{4}P$, qui pariter erit diuisor cuiusdam numeri formae $2aa+bb$.

Coroll.

Coroll. 2.

34. Proposito porro numero quocunque P, si inter numeros formae $2aa+bb$, minores quam $\frac{3}{4}PP$, nullus datur per P diuisibilis, tum etiam plane nullus existet numerus formae $2aa+bb$ per P diuisibilis.

Theorema 8.

35. Si numerus primus in forma $2aa+bb$ non contentus, fuerit diuisor cuiusquam numeri huius formae, neque radices seorsim per eum sint diuisibiles, tum alius quoque numerus primus, priore minor, et in hac forma non contentus, exhiberi poterit, qui etiam futurus sit diuisor cuiuspiam numeri eiusdem formae, neque tamen singulae radices per eum sint diuisibiles.

Demonstratio.

Demonstrandum ergo est, si fuerit numerus primus $\mathfrak{A}'$ diuisor cuiuspiam numeri $A=2aa+bb$, ita vt neque a, neque b per $\mathfrak{A}'$ sit diuisibile, tum quoque dari alium numerum primum $\mathfrak{B}'<\mathfrak{A}'$, qui quoque futurus sit diuisor numeri cuiuspiam $B=2cc+dd$, ita vt neque c, neque d, per illum sit diuisibile. Demonstrauimus autem, exhiberi posse numerum $A<\frac{3}{4}\mathfrak{A}'\mathfrak{A}'$; vnde si ponatur quotus $\frac{A}{\mathfrak{A}'}=Q$, erit $Q<\frac{3}{4}\mathfrak{A}'$, ideoque multo magis $Q<\mathfrak{A}'$. At per §. 31. vel hic ipse quotus Q erit numerus primus $\mathfrak{B}'$, vel saltem diuisorem habebit primum formae $\mathfrak{B}'$. Sit igitur vel ipse quotus Q, vel eius diuisor $=\mathfrak{B}$, qui certe mul-

to minor erit quam $\mathfrak{A}'$. Quare cum quotus Q sit diuisor numeri A, etiam $\mathfrak{B}'$ erit eius diuisor. Manifestum autem est, hunc quotum eiusue diuisorem $\mathfrak{B}'$ vnitatem esse non posse, cum vnitas non solum sit in forma $2aa+bb$ contenta; sed etiam in demonstratione Th. 6. excludatur. Q. E. D.

Coroll. 1.

36. Si ergo numeri cuiuspiam $A=2aa+bb$ diuisor esset numerus primus $\mathfrak{A}'$ in ista forma non contentus, neque a et b per eum seorsim fuerit diuisibile, tum alius quoque numerus primus illo minor $\mathfrak{B}'$ existeret diuisor numeri cuiuspiam $B=2cc+dd$.

Coroll. 2.

37. Cum autem A ita capi possit, vt sit $A<\frac{3}{4}\mathfrak{A}'\mathfrak{A}'$, ita etiam pro altero numero $\mathfrak{B}'$ inueniri poterit numerus $B<\frac{3}{4}\mathfrak{B}'\mathfrak{B}'$ per ea, quae in Theorem. 7. sunt demonstrata.

Coroll. 3.

38. Si numerus $A=2aa+bb$ fuerit diuisibilis per numerum primum $\mathfrak{A}'$, neque a et b per eum sint diuisibiles, numeri a et b pro primis inter se assumi poterunt: si enim haberent communem factorem, eo sublato nihilominus praeberent numerum $2aa+bb$ per $\mathfrak{A}'$ diuisibilem.

Coroll.

Coroll. 4.

39. At si numerus $A = 2aa + bb$, existentibus a et b inter se primis, diuisorem habeat $\mathfrak{A}'$, tum etiam numerus $B = 2cc + dd$ minor quam $\frac{3}{4}\mathfrak{A}'\mathfrak{A}'$ exhiberi poterit per $\mathfrak{A}'$ diuisibilis, ita vt c et d sint inter se primi. Posito enim $a = m\mathfrak{A}' \pm c$ et $b = n\mathfrak{A}' \pm d$ (32), numeri c et d certe non erunt per $\mathfrak{A}'$ diuisibiles, ac si quem alium habeant communem factorem, puta $e = kp$ et $d = kq$, etiam $2pp + qq$ per $\mathfrak{A}'$ erit diuisibilis, existentibus p et q inter se primis: hocque casu multo magis $2pp + qq$ minus erit quam $\frac{3}{4}\mathfrak{A}'\mathfrak{A}'$.

Coroll. 5.

40. Cum igitur existente $A = 2aa + bb$ diuisibili per $\mathfrak{A}'$, et radicibus a et b inter se primis, exhiberi possit numerus $B = 2cc + dd$ minor quam $\frac{3}{4}\mathfrak{A}'\mathfrak{A}'$, ita vt c et d sint numeri inter se primi, qui sit quoque per $\mathfrak{A}'$ diuisibilis, erit, vt vidimus, hic idem numerus B quoque per alium numerum primum $\mathfrak{B}' < \frac{3}{4}\mathfrak{A}'$ diuisibilis.

Coroll. 6.

41. Atque cum $B = 2cc + dd$, existentibus c et d numeris inter se primis, iam sit diuisibilis per numerum primum $\mathfrak{B}'$ minorem quam $\mathfrak{A}'$, inde nouus numerus $C = 2ee + ff$ per $\mathfrak{B}'$ quoque diuisibilis inveniri poterit, ita vt e et f sint numeri primi inter se, et ipse numerus C minor quam $\frac{3}{4}\mathfrak{B}'\mathfrak{B}'$.

Theorema 9.

42. Nullus datur numerus formae $2aa+bb$, existentibus a et b numeris inter se primis, qui diuisibilis sit per vllum numerum primum in ista forma non contentum.

Demonstratio.

Fingamus enim, per numerum primum $\mathfrak{A}'$ diuisibilem esse numerum $A=2aa+bb$, atque a et b esse numeros inter se primos: hicque numerus A, si non minor fuerit quam $\frac{3}{4}\mathfrak{A}'\mathfrak{A}'$, in minórem transformari poterit. Habebit autem tum hic numerus A alium diuisorem primum in forma $2aa+bb$ non contentum, qui sit $=\mathfrak{B}'$, eritque $\mathfrak{B}'<\frac{3}{4}\mathfrak{A}'$, ad si fuerit $A>\frac{3}{4}\mathfrak{B}'\mathfrak{B}'$ reperietur nouus numerus $B=2cc+dd$ diuisibilis per $\mathfrak{B}'$, ita vt c et d sint numeri inter se primi $B<\frac{3}{4}\mathfrak{B}'\mathfrak{B}'$. Iam simili modo, cum B habeat diuisorem $\mathfrak{B}'$, alium praeterea habebit diuisorem eiusdem indolis $\mathfrak{C}'<\frac{3}{4}\mathfrak{B}'$, hincque porro nouus numerus $C=2ee+ff$ per $\mathfrak{C}'$ diuisibilis reperietur, vt sit $C<\frac{3}{4}\mathfrak{C}'\mathfrak{C}'$, et e et f, numeri primi inter se. Hoc modo procedendo continuo minores numeri formae $2aa+bb$ obtinerentur, qui diuisibiles essent per numeros in forma $2aa+bb$ non contentos. Quare cum in minoribus numeris formae $2aa+bb$, siquidem a et b sint primi inter se, nullus occurrat, qui habeat diuisorem in forma ista non contentum, ne in maximis quidem huiusmodi numeri existunt, atque idcirco nullus plane datur numerus formae $2aa+bb$, qui sit diui-

diuisibilis per vllum numerum in ea forma non contentum, siquidem a et b sint primi inter se. Q. E. D.

Coroll. 1.

43. Iam ergo euicta est veritas obseruationis quintae, qua animaduertimus, numerum quemcunque formae $2aa+bb$, siquidem a et b sint numeri primi inter se, nullos alios habere diuisores primos, nisi qui sint eiusdem formae.

Coroll. 2.

44. Omnis ergo numerus formae $2aa+bb$, siquidem a et b sint primi inter se, vel ipse est primus, vel est productum ex duobus pluribusue numeris primis, qui omnes in forma $2aa+bb$ contineantur. Huiusmodi itaque numerus nullos alios admittit diuisores, nisi qui sint eiusdem formae $2aa+bb$.

Coroll. 3.

45. Nullus ergo numerus primus in forma $2aa+bb$ non contentus, cuiusmodi sunt 5, 7, 13, 23, 29, 31, 37, 47, 53, etc. vnquam diuisor, vel factor, esse poterit vllius numeri formae $2aa+bb$, siquidem a et b sint numeri primi inter se. Neque vero hac restrictione, quod numeri a et b inter se primi esse debeant, est opus, dummodo vterque non sit per illum numerum primum diuisibilis. Si enim a et b communem habeant diuisorem n, per illum numerum primum non diuisibilem, vt sit $a=nc$ et $b=nd$, tum quia $2cc+dd$ non est diuisibilis, neque etiam $nn(2cc+dd)$, seu $2aa+bb$, per illum erit diuisibilis.

Scholion.

46. Notetur probe vis huius demonstrationis, quae omnino est singularis, et in hoc consistit, quod in minoribus numeris nullus reperiatur numerus formae $2aa+bb$, existentibus a et b numeris inter se primis, qui sit diuisibilis per vllum numerum primum in ista forma $2mm+nn$ non contentum. Hinc enim concluſi, etiam ne in maioribus et maximis quidem numeris nullos dari per eiusmodi numeros primos diuisibiles. Demonstraui enim si in maximis tales darentur numeri, tum etiam inter minores, ac tandem minimos, futuros esse numeros eiusdem indolis. Neque vero opus est ad hanc demonstrationem nosse, in numeris minimis nullos dari numeros formae $2aa+bb$, per numerum primum, qui non sit eiusdem formae, diuisibiles; hoc enim ipsum iam per se est absurdum, minores continuo exhiberi posse numeros formae $2aa+bb$, qui per numerum primum non eiusdem formae essent diuisibiles. Namque tandem necessario perueniri oporteret ad numeros primos, qui cum sint formae $2aa+bb$, certe per nullum numerum primum a se diuersum dividi possent. Quare si de quacunque alia forma $maa+bb$, existentibus a et b numeris inter se primis, demonstrari posset, quod si maiores numeri eius formae dentur per numerum primum non eiusdem formae diuisibiles, tum etiam necessarios minores dari numeros, qui quoque numerum primum non eiusdem formae futuri sint diuisibiles, tum tuto concludere possemus, nullos plane dari numeros formae $maa+bb$, qui per vllum numerum primum in eadem forma non con-

contentum sint diuisibiles. Verum vt similis demonstratio locum habere possit, necesse est, vt $\frac{m+2n}{4}$ non sit maius quam 1, alias enim theorema 7 et 8 applicari non posset: vnde huiusmodi demonstratio non valebit, nisi in formis $aa+bb$, $2aa+bb$ et $3aa+bb$. At in hac postrema quidem forma exceptionem facit diuisor 2 in forma $3aa+bb$ non contentus; hoc enim casu fit $a=1$, et $b=1$, seu $3.1+1$ est forma simplicissima per 2 diuisibilis, quae cum non sit minor, quam 2^2, quotus quoque non minor prodit quam 2; ideoque hinc conclusio ad numerum primum minorem in forma $3aa+bb$ non contentum, non succedit.

Theorema 10.

47. Si numerus formae $2aa+bb$ vnico modo in hanc formam fuerit resolubilis, atque a et b fuerint primi inter se, tum ille numerus certo est primus.

Demonstratio.

Si enim non esset primus, duos pluresue haberet factores primos formae $2aa+bb$, ideoque duobus pluribusue modis in formam $2aa+bb$ esset resolubilis, vt in theoremate 3 demonstrauimus; pluralitas enim resolutionum in dubium vocari nequit, si factores illi, quos habent, fuerint inaequales. Verum etiamsi factores fuerint aequales, tamen resolutio plus vno modo succedit: nam si numerus propositus N sit $=(2aa+bb)^2$ erit I. $N=2.0^2+(2aa+bb)^2$ et II. $N=2(2ab)^2+(2aa-bb)^2$ at si sit $N=(2aa+bb)^3$, erit

I. N=

I. $N = 2(2a^3 + abb)^2 + (2aab + b^3)^2$

II. $N = 2(2a^3 - 3abb)^2 + (6aab - b^3)^2$

Porro si sit $N = (2aa + bb)^4$ erit quoque:

I. $N = 2.0^2 + (4a^4 + 4aabb + b^4)^2$

II. $N = 2(4a^3b + 2ab^3)^2 + (4a^4 - b^4)^2$

III. $N = 2(8a^3b - 4ab^3)^2 + (4a^4 - 12aabb + b^4)^2$

Ergo pluralitas resolutionum etiam locum habet, si factores fuerint aequales, dummodo resolutiones, quibus vel altera radix euanescit, vel ambae communem habeant diuisorem, non excludantur. Hinc ergo patet, si numerus $2aa + bb$, existentibus a et b numeris primis inter se, vnico modo fuerit resolubilis in hanc formam, tum eum certo esse primum. Q. E. D.

Coroll. 1.

48. Proposito ergo numero quocunque, quem constat esse in forma $2aa + bb$ contentum, facile erit explorare, vtrum sit primus, nec ne? Considerentur enim numeri a et b, qui si non fuerint primi inter se, statim habetur factor, sin autem sint primi, tum inde successiue omnia quadrata duplicata $2aa$ subtrahentur, et dispiciatur, an vsquam quadratum bb relinquatur, quod si praeter casum cognitum non eueniat, certo pronunciare poterimus, numerum propositum esse primum.

Coroll. 2.

49. Sin autem numerus propositus plus vno modo in quadratum et duplum quadratum fuerit resolubilis,

bilis, tum non solum nouimus eum non esse primum, sed etiam eius factores assignare poterimus, secundum ea, quae §. 21. sunt tradita. Hic autem modus numeros examinandi satis expedite perfici potest, perinde atque ego iam ex natura summae duorum quadratorum similem modum exposui.

Theorema II.

50. Nullus numerus, qui vel in hac forma $8n-1$, vel in hac $8n-3$ continetur, diuidere potest vllum numerum formae $2aa+bb$, siquidem a et b sint numeri primi inter se.

Demonstratio.

Demonstrasse sufficiet, nullum numerum, vel formae $8n-1$, vel $8n-3$, vnquam esse posse formae $2aa+bb$; cum enim haec forma $2aa+bb$ nullos alios admittat diuisores, nisi qui in hac ipsa forma sint contenti, statim ac demonstrauerimus, nullum numerum, vel formae $8n-1$, vel $8n-3$, in forma $2aa+bb$ contineri, simul certum erit, ne quidem diuisorem huius formae esse posse. Cum autem $8n-1$ et $8n-3$ sint numeri impares, videamus, quibus casibus forma $2aa+bb$ numeros impares producat: manifestum autem est, hoc fieri non posse, nisi b sit numerus impar; quo casu bb fiet numerus formae $8m+1$. Tum vero numerus a vel erit par, vel impar; priori casu erit aa formae $4n$, ideoque $2aa$ formae $8n$, vnde expressio $2aa+bb$ abibit in numerum formae $8m+8n+1$, seu $8n+1$.

Posteriori casu, quo a est numerus impar, erit aa numerus formae $4n+1$, ideoque $2aa$ formae $8n+2$, vnde expressio $2aa+bb$ praebet hoc casu numerum formae $8m+1+8n+2$, seu formae $8n+3$. Forma ergo $2aa+bb$ alios numeros impares non continet, nisi qui fuerint, vel formae $8n+1$, vel formae $8n+3$. Quare nullus numerus impar, vel formae $8n-1$, vel formae $8n-3$, vnquam in forma $2aa+bb$ continetur, nec propterea vllius numeri $2aa+bb$ diuisor existere potest, si quidem a et b sint numeri primi inter se. Q. E. D.

Coroll. 1.

51. Si ergo a et b fuerint numeri primi inter se, numerus $2aa+bb$ nunquam erit diuisibilis, vel per 5, vel per 7, vel per vllum numerum huius seriei 5, 7, 13, 23, 29, 31, 37, 47, 53, 61, 71, 79, etc. neque etiam per vllum numerum non primum, vel in forma $8n-1$, vel in forma $8n-3$, contentum, quales sunt 15, 21, 35, 39, 45, 63, 69, 77, 85, 87, 93, 93, 95 etc.

Coroll. 2.

52. Omnes ergo numeri impares, qui vnquam esse possunt diuisores numerorum formae $2aa+bb$, siquidem a et b sint inter se primi, vel in hac formula $8n+1$, vel hac $8n+3$, continentur. Neque tamen vlli numeri compositi harum formularum, qui factores habent formae $8n-1$, vel $8n-3$, diuisores numeri $2aa+bb$ existere possunt.

Coroll.

Coroll. 3.

53. Etiamsi ergo producta $(8m-1)(8n-1)$, $(8m-1)(8n-3)$, et $(8m-3)(8n-3)$ in formis $8m+1$ vel $8m+3$ contineantur, tamen ea nunquam diuisores vllius numeri formae $2aa+bb$ existere possunt, si quidem a et b fuerint numeri primi inter se.

Coroll. 4.

54. Quoties ergo forma $2aa+bb$ sit numerus primus, is semper vel in hac numerorum serie $8n+1$, vel hac $8n+3$, continebitur; vnde in his duabus seriebus etiam omnes diuisores primi, vel saltem impares numerorum in formula $2aa+bb$ contentorum, reperientur.

Scholion 1.

55. Vtrum autem omnes numeri primi, qui in seriebus numerorum $8n+1$ et $8n+3$ occurrunt, vicissim sint numeri formae $2aa+bb$, quaestio est altioris indaginis. Quousque quidem supra numeros primos formae $2aa+bb$ continuauimus, vidimus in illis omnes plane numeros primos, tam huius formae $8n+1$, quam huius $8n+3$, occurrere, vnde omnes quoque numeri primi in his duabus formulis contenti, simul in forma $2aa+bb$ contineri videntur: verum huius veritatis demonstratio maxime est abstrusa. Viam tamen ad eam iam non parum praeparauimus, dum demonstrauimus, omnes diuisores formae $2aa+bb$ simul esse numeros eiusdem formae, siquidem a et b fuerint inter se primi: nam proposito numero primo quocunque

primo P sive formae $8n+1$, sive $8n+3$, si demonstrare potuerimus, dari quempiam numerum $2aa+bb$ per illum diuisibilem, ita vt neque a, neque b, per eum sit diuisibile; simul erit certum, numerum P esse in forma $2mm+nn$ contentum.

Scholion 2.

56. Quod autem omnis numerus primus in altervtra harum formularum $8n+1$ et $8n+3$ necessario sit aggregatum ex quadrato et duplo quadrato, vti id in numeris minoribus 500 non superantibus euenire vidimus, equidem me nondum demonstrare posse, fateor. haecque demonstratio multo magis ardua videtur, quam ea, qua probaui, omnem numerum primum formae $4n+1$ esse summam duorum quadratorum. Cum autem momentum in hoc versetur, vt demonstretur, proposito quocunque numero primo, vel formae $8n+1$, vel formae $8n+3$, semper dari numerum $2aa+bb$ per eum diuisibilem, ita vt radices a et b sint numeri inter se primi, operam is perdiderit, qui valores numerorum a et b per n expressos, inuestigare voluerit, propterea quod hi numeri non tantum ab n pendent, sed etiam ea ratio, quod numerus $8n+1$ vel $8n+3$ sit primus, necessario in computum duci debeat. Nam si numerus $8n+1$, vel $8n+3$, non fuerit primus, euenire adeo potest, vt nullus numerus $2aa+bb$ per eum sit diuisibilis. Iam equidem demonstraui, per numerum $8n+1$, si sit primus, diuisibiles esse omnes numeros formae $p^{4n}-q^{4n}$, et per numerum

merum primum $8n+3$ omnes numeros formae $p^{8n+2} - q^{8n+2}$; tum vero etiam semper eiusmodi dari numeros p et q, vt priori casu forma $p^{4n}+q^{4n}$ per $8n+1$, posteriori vero forma $p^{4n+1}+q^{4n+1}$ per $8n+3$ diuisibilis existat. Demonstrandum igitur esset, in his formis $p^{4n}+q^{4n}$ et $p^{4n+1}+q^{4n+1}$ necessario semper eiusmodi inuolui casus, qui sint aggregata ex quadrato et duplo quadrato; quod autem quo modo demonstrari posset, nondum perspicio. Aeque difficile ergo, ac fortasse difficilius erit, sequentes propositiones demonstrare, quae tamen aeque certae videntur, excepta prima, cuius demonstrationem dedi.

I. Omnis numerus primus formae $4n+1$ in hac forma $aa+bb$ continetur.

II. Omnes numeri primi in his formis $8n+1$ et $8n+3$ contenti, simul in hac forma continentur $2aa+bb$.

III. Omnes numeri primi vel huius formae $12n+1$, vel huius $12n+7$, seu huius vnicae $6n+1$, in hac forma $3aa+bb$ continentur.

IV. Omnes numeri primi in quapiam harum formularum

$16n+1$, $16n+5$, $16n+9$, $16n+13$,

vel in hac $4n+1$ contenti, simul sunt numeri formae $4aa+bb$, cuius quidem demonstratio iam in prima comprehenditur.

V. Omnes numeri primi in aliqua harum formularum contenti

$20n+1$; $20n+9$;

simul quoque sunt formae $5aa+bb$.

VI. Omnes numeri primi in aliqua harum formularum contenti,

$24n+1$; $24n+7$;

simul quoque sunt formae $6aa+bb$.

VII. Omnes numeri primi in aliqua harum formularum contenti,

$28n+1$; $28n+9$; $28n+11$; $28n+15$; $28n+23$; $28n+25$,

vel, quod eodem redit, in harum aliqua:

$14n+1$; $14n+9$; $14n+11$;

simul quoque sunt formae $7aa+bb$.

VIII. Omnes numeri primi in alterutra harum formularum contenti,

$24n+5$ et $24n+11$;

simul sunt numeri formae $3aa+2bb$.

Huiusmodi autem theorematum numerus quousque libuerit continuari potest.

Verum tamen in iis formandis probe cauendum est, ne inductioni nimis tribuatur: neque enim si fuerit numerus quispiam primus p in hac forma $faa+gbb$ contentus, inde generatim concludere licet, omnes numeros primos forma $4fgn+p$ fore numeros eiusdem formae $faa+gbb$, etiamsi hoc, si f et g fuerint numeri exigui, verum esse videatur. Etsi enim est $67=5.9$

$+22$.

$+22.1$, ideoque formae $5aa+22bb$, tamen numerus $4.5.22n+67$, casu $n=2$, qui est $=40.22+67=947$ scilicet primus, non in forma $5aa+22bb$ continetur: interim tamen affirmare licet, cum sit $23=5.2^2+3.1$, ideoque in forma $5aa+3bb$ contineatur, omnes numeros primos $60n+23$ in eadem forma contineri. Quodsi igitur, quis methodum inuenerit, huiusmodi theoremata tam inueniendi, quam, in quo caput rei est positum, demonstrandi, is certe in doctrina numerorum plurimum praestitisse erit iudicandus.

Admissa autem hac proprietate numerorum primorum in his formulis $8n+1$ et $8n+3$ contentorum, plura alia hinc deduci poterunt egregia Theoremata, quorum quaedam notasse iuuabit.

Theorema 12.

57. Si numerus quicunque in alterutra harum formularum $8n+1$, vel $8n+3$, contentus, nullo modo in formam $2aa+bb$ resolui possit, tum non erit primus; at si vnico modo in hanc formam possit resolui, tum erit primus: sin autem plus vno modo haec resolutio succedat, tum pariter non erit primus, sed compositus.

Demonstratio.

Pars secunda et tertia ex iam demonstratis sunt manifestae. Si enim numerus propositus vnico modo in forma $2aa+bb$ continetur, tum certe est primus, sin pluribus, compositus. Quod autem ad partem primam

mam attinet, ea vi proprietatis nondum demonstratae subsistit; nam si numerus propositus esset primus, in formam $2aa+bb$ resolui posset, quando ergo hanc resolutionem non admittit, tum certo non est primus. Q. E. D.

Corollarium. 1.

58. Hinc igitur patet modus non difficilis propositum numerum, si fuerit, vel formae $8n+3$, vel $8n+1$, explorandi, vtrum sit primus, nec ne? Subtrahantur enim ab eo successiue omnia quadrata duplicata, scilicet:

2, 8, 18, 32, 50, 72, 98 etc.

quorum differentiae constituunt progressionem arithmeticam:

6, 10, 14, 18, 22, 26, etc.

et dispiciatur, vtrum vspiam quadratum relinquatur.

Coroll. 2.

59. Possunt etiam plures operationes simul institui, ac primo successiue subtrahi haec quadrata duplicata:

2, 72, 242, 512, 882 etc. quorum differentiae sunt 70, 170, 270, 370, etc.

secundò vero haec quadrata duplicata:

8, 98, 288, 578, 968 etc. quorum differentiae sunt 90, 190, 290, 390, etc.

tertio

tertio haec:

18, 128, 338, 648, 1058 etc. quorum differentiae sunt
110, 210, 310, 410 etc.

quarto haec:

32, 162, 392, 722, 1152 etc. quorum differentiae sunt
130, 230, 330, 430 etc.

quinto haec:

50, 200, 450, 800, 1250 etc. quorum differentiae sunt
150, 250, 350, 450 etc.

vbi ex figuris finalibus mox patebit, quaenam operationes sint inutiles.

Coroll. 3.

60. A numeris autem formae $8n+1$, quadrata tantum paria duplicata subtrahi debent, vnde exclusis quadratis imparibus duplicatis, sequentes numeri erunt subtrahendi:

I. 8, 288, 968, 2048 etc. 280, 680, 1080 400, 400	II. 32, 392, 1152, 2312 etc. 360, 760, 1160 400, 400
III. 0, 200, 800, 1800 etc. 200, 600, 1000 400, 400	IV. 72, 512, 1352, 2592 etc. 440, 840, 1240 400, 400

V. 128, 648, 1568, 2888 etc.
520, 920, 1320
400, 400

Coroll. 4.

61. Sin autem numerus sit formae $8n+3$, tum tantum quadrata imparia duplicata subtrahi debent, quae sunt:

I. 2, 242, 882, 1922 etc.	II. 18, 338, 1058, 2178 etc.
240, 640, 1040	320, 720, 1120
400, 400	400, 400
III. 50, 450, 1250, 2450 etc.	IV. 98, 578, 1458, 2738 etc.
400, 800, 1200	480, 880, 1280
400, 400	400, 400

V. 162, 722, 1682, 3042 etc.
560, 960, 1360
400, 400

Exemplum 1.

62. Exploretur numerus 67579, vtrum sit primus, nec ne?

Cum hic numerus contineatur in forma $8n+3$, subtrahantur numerorum ordines ex coroll 4, isque tantum secundus, tertius ac quartus, quia primus et quintus darent notam finalem 7, quae quadrato repugnat:

II.	67579	53801	III.	67579	53129	IV. 67579	52441 * 229
	18	3520		50	3600	98	3680
	67561	50281		67529	49529	67481	45761
	320	3920		400	4000	480	4080
	67241	46361		67129	45529	67001	44681
	720	4320		800	4400	880	4480
	66521	42041		66329	41129	66121	40201
	1120	4720		1200	4800	1280	4880
	65401	37321		65129	36329	64841	35321
	1520	5120		1600	5200	1680	5280
	63881	32201		63529	31129	63161	30041
	1920	5520		2000	5600	2080	5680
	61961	26681		61529	25529	61081	24361
	2320	5920		2400	6000	2480	6080
	59641	20761		59129	19529	58601	18281
	2720	6320		2800	6400	2880	6480
	56921	14441		56329	13129	55721	11801
	3120	6720		3200	6800	3280	6880
	53801	7721		53129	6329	52441	4921
		7120					
		601					

Hic vnicum occurrit quadratum $52441 = 229^2$, vt sit $67579 = 2.87^2 + 229^2$, ideoque primus.

Exemplum 2.

63. Exploretur numerus 40081, vtrum sit primus, nec ne?

Cum hic numerus contineatur in forma $8n+1$, subtrahantur numeri Coroll. 3 eorumque quidem ordines II, III et IV, hoc modo:

II.		III.		IV.	
40081	29129	40081	30281	40081	31369
32	3160	200	3000	72	2840
40049	25969	39881	27281	40009	28529
360	3560	600	3400	440	3240
39689	22409	39281	23881	39569	25289
760	3960	1000	3800	840	3640
38929	18449	38281	20081	38729	21649
1160	4360	1400	4200	1240	4040
37769	14089	36881	15881	37489	17609
1560	4760	1800	4600	1640	4440
36209	9329	35081	11281	35849	13169
1960	5160	2200	5000	2040	4840
34249	4169	32881	6281	33809	8329
2360		2600	5400	2440	5240
31889		30281	881	31369	3089
2760					
29129					

quia igitur hic nusquam quadratum remansit, numerus propositus non est primus, est vero productum $= 149 . 269$.

Theorema 13.

64. Si numerus n nullo modo sit aggregatum ex numero quadrato et trigonali, tum numerus $8n+1$ certe non erit primus.

Demon-

Demonstratio.

Si enim n nullo modo in hac forma $aa+\frac{1}{2}(bb+b)$ continetur, tum $8n+1$ nullo modo in hac forma $8aa+4bb+4b+1$ continetur, non ergo erit numerus formae $2pp+qq$, ideoque non erit primus. Q. E. D.

Corollarium.

65. At si n vnico modo sit aggregatum ex quadrato et trigonali, tum $8n+1$ certe erit numerus primus, sin autem sit pluribus modis, non erit primus, sed compositus.

Theorema 14.

66. Si numerus n nullo modo fuerit aggregatum ex numero trigonali et trigonali duplicato, tum $8n+3$ certe non erit primus.

Demonstratio.

Si enim n nullo modo in hac forma $aa+a+\frac{1}{2}(bb+b)$ contineatur, tum $8n+3$ nullo modo in hac forma $8aa+8a+2+4bb+4b+1$, ideoque nec in hac $2pp+qq$ continebitur, consequenter non erit primus. Q. E. D.

Corollarium.

67. At si n vnico modo fuerit aggregatum ex trigonali et trigonali duplicato, tum $8n+3$ certe erit primus, sin autem fuerit plus vno modo, compositus.

PHY-