1750

Theoremata circa divisores numerorum

Leonhard Euler

THEOREMATA
CIRCA DIVISORES NVMERORVM.

AVCTORE
L. EVLERO.

Quouis tempore ſummi Geometrae agnouerunt in natura numerorum plurimas praeclariſſimas proprietates eſſe abſconditas, quarum cognitio fines matheſeos non mediocriter eſſet amplificatura. Primo quidem intuitu doctrina numerorum ad arithmeticae elementa referenda videtur, atque vix quicquam in ea ineſſe putatur, quod vllam ſagacitatem aut vim analyſeos requirat. Qui autem diligentius in hoc genere ſunt verſati, non ſolum veritates demonſtratu difficillimas detexerunt, ſed etiam eiusmodi, quarum certitudo percipiatur, etiamſi demonſtrari nequeat. Plurima huiusmodi theoremata ſunt prolata ab inſigni Geometra Fermatio, quorum veritas quamuis demonſtratio lateat, non minus euicta videtur. Atque hoc imprimis omnem attentionem meretur, in matheſi adeo pura eiusmodi dari veritates, quas nobis cognoscere liceat, cum tamen eas demonſtrare non valeamus; atque hoc adeo in arithmetica vſu venit, quae tamen prae reliquis matheſeos partibus maxime pertractata ac perſpecta haberi ſolet: neque facile affirmare auſim, an ſimiles veritates in reliquis partibus reperiantur. In Geometria certe nulla occurit propoſitio cuius vel veritas vel falſitas firmiſſimis rationibus euinci nequeat. Cum igitur quaeuis veritas eo magis abſtruſa cenſeatur, quo minus ad eius demonſtrationem

onem aditus pateat, in arithmetica certe, vbi natura numerorum perpenditur, omnium abſtruſiſſimas contineri negare non poterimus. Non deſunt quidem inter ſummos mathematicos Viri, qui huiusmodi veritates prorſus ſteriles, ideoque non dignas iudicant, in quarum inueſtigatione vlla opera collocetur; at praeterquam quod cognitio omnis veritatis per ſe ſit excellens, etiamſi ab vſu populari abhorere videatur, omnes veritates, quas nobis cognoſcere licet, tantopere inter ſe connexae deprehenduntur, vt nulla ſine temeritate tanquam prorſus inutilis repudiari poſſit. Deinde etſi quaepiam propoſitio ita comparata videatur, vt ſiue vera ſit ſiue falſa, nihil inde ad noſtram vtilitatem redundet, tamen ipſa methodus, qua eius veritas vel falſitas euincitur, plerumque nobis viam ad alias vtiliores veritates cognoſcendas pateſacere ſolet. Hanc obrem non inuiliter me operam ac ſtudium in indagatione demonſtrationum quarumdam propoſitionum impendiſſe confido, quibus inſignes circa diuiſores numerorum proprietates continentur. Neque vero haec de diuiſoribus doctrina omni caret vſu, ſed nonnunquam in analyſi non contemnendam praeſtat vtilitatem. Imprimis vero non dubito, quin methodus ratiocinandi, qua ſum vſus, in aliis grauioribus inueſtigationibus aliquando non parum ſubſidii afferre poſſit. Propoſitiones autem, quas hic demonſtratas exhibeo, reſpiciunt diuiſores numerorum in hac formula $a^n \pm b^n$ contentorum, quarum nonnullae iam ab ante memorato Fermatio, ſed ſine demonſtratione, ſunt publicatae. Quoniam igitur hic perpetuo de numeris integris ſermo inſtituetur, omnes alphabeti litterae hic conſtanter numeros integros indicabunt.

Theo-

Theorema I.

1. Si p fuerit numerus primus, omnis numerus in hac forma $(a+b)^p - a^p - b^p$ contentus diuiſibilis erit per p.

Demonſtratio.

Si binomium $(a+b)^p$ modo conſueto euoluatur, erit $(a+b)^p = a^p + \frac{p}{1} a^{p-1} b + \frac{p(p-1)}{1 \cdot 2} a^{p-2} b^2 + \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3} a^{p-3} b^3 + \ldots + \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3} a^3 b^{p-3} + \frac{p(p-1)}{1 \cdot 2} a^2 b^{p-2} + \frac{p}{1} a b^{p-1} + b^p$. qua expreſſione ſubſtituta, binisque terminis, qui easdem habent vncias, coniunctis, erit $(a+b)^p - a^p - b^p = \frac{p}{1} ab(a^{p-2} + b^{p-2}) + \frac{p(p-1)}{1 \cdot 2} a^2 b^2 (a^{p-4} + b^{p-4}) + \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3} a^3 b^3 (a^{p-6} + b^{p-6}) + \frac{p(p-1)(p-2)(p-3)}{1 \cdot 2 \cdot 3 \cdot 4} (a^{p-8} + b^{p-8}) a^4 b^4 +$ etc. Hic primo notandum eſt omnes vncias, quamquam ſub forma fractionum apparent, nihilominus eſſe numeros integros, cum exhibeant, vti conſtat numeros figuratos. Quaelibet ergo vncia cum factorem habeat p, diuiſibilis erit per p, niſi is alicubi per factorem denominatoris vel prorſus tollatur, vel diuidatur. At vbique omnes factores denominatorum minores ſunt quam p quia adeo non vltra $\frac{1}{2}p$ creſcunt, ideoque factor numeratorum p nusquam per diuiſionem tollitur. Deinde cum p ſit per hypoth. numerus primus, is nusquam per diuiſionem minuetur. Quocirca ſingulae vnciae $\frac{p}{1}$; $\frac{p(p-1)}{1 \cdot 2}$; $\frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3}$; etc. hincque tota expreſſio $(a+b)^p - a^p - b^p$ perpetuo per numerum p ſiquidem fuerit numerus primus, erit diuiſibilis Q. E. D.

Coroll.

Coroll. 1.

2. Si ergo ponatur $a=1$, et $b=1$, erit 2^p-2 semper diuisibilis per p, si quidem fuerit p numerus primus. Cum igitur sit $2^p-2=2(2^{p-1}-1)$: alterum horum factorum per p diuisibilem esse oportet. At nisi sit $p=2$, prior factor 2 per p non est diuisibilis: vnde sequitur formam $2^{p-1}-1$ perpetuo per p esse diuisibilem, si p fuerit numerus primus praeter binarium.

Coroll. 2.

3. Ponendis ergo pro p successiue numeris primis, erit 2^2-1 diuisibile per 3; 2^4-1 per 5; 2^6-1 per 7; $2^{10}-1$ per 11 etc. quod in minoribus numeris per se fit perspicuum, in maximis autem aeque erit certum. Sic cum 641 sit numerus primus, iste numerus $2^{640}-1$ necessario per 641 erit diuisibilis. Seu si potestas 2^{640} per 641 diuidatur, post diuisionem supererit residuum $=1$.

Theorema 2.

4. Si vtraque harum formularum a^p-a et b^p-b fuerit diuisibilis per numerum primum p, tum quoque ista formula $(a+b)^p-a-b$ diuisibilis erit per eundem numerum primum p.

Demonstratio.

Cum per §. 1. $(a+b)^p-a^p-b^p$ sit diuisibilis per numerum p, si fuerit primus, atque hic formulae a^p-a et b^p-b per p diuisibiles assumantur, erit quoque summa istarum trium formularum nempe $(a+b)^p-a-b$ per p, si fuerit numerus primus diuisibilis Q. E. D.

Coroll.

Coroll. 1.

5. Si ponatur $b=1$, cum $1^p-1=0$ ſit diuiſibile per p; ſequitur, ſi formula a^p-a fuerit diuiſibilis per p, tum quoque formulam $(a+1)^p-a-1$ fore per p diuiſibilem.

Coroll. 2.

6. Cum igitur aſſumta formula a^p-a per p diuiſibili, ſit quoque formula $(a+1)^p-a-1$ per p diuiſibilis; ſimili modo in eadem hyphotheſi erit haec quoque formula $(a+2)^p-a-2$, hincque porro haec $(a+3)^p-a-3$, etc. atque generaliter haec c^p-c diuiſibilis per p.

Theorema 3.

7. Si p fuerit numerus primus, omnis numerus huius formae c^p-c per p erit diuiſibilis.

Demonſtratio.

Si in §. 6 ponatur $a=1$, cum ſit $a^p-a=0$ per p diuiſibilis, ſequitur has quoque formulas 2^p-2; 3^p-3; 4^p-4; etc. et generatim hanc c^p-c fore per numerum primum p diuiſibilem. Q. E. D.

Coroll. 1.

8. Quicunque ergo numerus integer pro c aſſumatur, denotante p numerum primum, omnes numeri in hac forma c^p-c contenti erunt diuiſibiles per p.

Coroll. 2.

9. Cum autem ſit $c^p-c=c(c^{p-1}-1)$, vel ipſe numerus c vel $c^{p-1}-1$ diuiſibilis erit per p: vtrumque autem

autem ſimul per p diuiſibilem eſſe non poſſe manifeſtum eſt. Quare ſi numerus c non fuerit diuiſibilis per p, haec forma $c^{p-1}-1$ certe per p erit diuiſibilis.

Coroll. 3.

10. Si ergo p fuerit numerus primus, omnes numeri in hac forma contenti $a^{p-1}-1$ erunt diuiſibiles per p exceptis iis caſibus, quibus ipſe numerus a per p eſt diuiſibilis.

Theorema 4.

11. Si neuter numerorum a et b diuiſibilis fuerit per numerum primum p, tum omnis numerus huius formae $a^{p-1}-b^{p-1}$ erit diuiſibilis per p.

Demonſtratio.

Cum neque a neque b ſit diuiſibilis per p, atque p denotet numerum primum, tam haec forma $a^{p-1}-1$, quam haec $b^{p-1}-1$ erit diuiſibilis per p. Hinc ergo quoque differentia iſtarum formularum $a^{p-1}-b^{p-1}$ erit diviſibilis per p. Q. E. D.

Coroll. 1.

12. Cum omnis numerus primus praeter binarium, cuius ratio diuidendi per ſe eſt manifeſta, ſit impar, ponatur $2m+1$ pro p, atque perſpicuum erit, omnes numeros in hac forma $a^{2m}-b^{2m}$ contentos eſſe diuiſibiles per p $2m+1$, ſiquidem neque a neque b ſeorſim fuerit per $2m+1$ diuiſibilis.

Coroll. 2.

13. Quia b non eſt diuiſibilis per $2m+1$, etiam

b^{2m} et $2b^{2m}$ non diuiſibile erit per $2m+1$. Quare ſi $2b^{2m}$ addatur ad formulam $a^{2m}-b^{2m}$, quae eſt diuiſibilis per $2m+1$, prodibit formula $a^{2m}+b^{2m}$, quae per $2m+1$ non erit diuiſibilis; niſi vterque numerus a et b ſeorſim per $2m+1$ ſit diuiſibilis.

Coroll. 3.

14. Quoniam ob $2m$ numerum parem formula $a^{2m}-b^{2m}$ factores habet $(a^m-b^m)(a^m+b^m)$, neceſſe eſt vt horum factorum alter ſit diuiſibilis per $2m+1$: ambo autem ſimul per numerum $2m+1$ diuiſibiles eſſe nequeunt. Quare ſi $2m+1$ fuerit numerus primus, et neque a neque b diuiſibile ſit per $2m+1$, tum vel a^m-b^m vel a^m+b^m erit diuiſibile per $2m+1$.

Coroll. 4.

15. Si m ſit numerus par puta $=2n$, atque a^m-b^m ſeu $a^{2n}-b^{2n}$ diuiſibilis per $2m+1=4n+1$, tum ob eandem rationem vel a^n-b^n vel a^n+b^n diviſibile erit per numerum primum $4n+1$.

Theorema 5.

16. Summa duorum quadratorum $aa+bb$ per nullum numerum primum huius formae $4n-1$ vnquam diuidi poteſt, niſi vtriusque radix ſeorſim a et b ſit diuiſibilis per $4n-1$.

Demonſtratio.

Si $4n-1$ fuerit numerus primus, neque a et b per illum ſint diuiſibiles, tum $a^{4n-2}-b^{4n-2}$ erit diuiſibile per $4n-1$ (11), hincque iſta formula $a^{4n-2}+b^{4n-2}$ non erit diuiſi-

diuiſibilis per $4n-1$, neque propterea vllus eius factor. At cum $4n-2=2(2n-1)$ ſit numerus impariter par, formula $a^{4n-2}+b^{4n-2}$ factorem habet $aa+bb$; quare fieri nequit, vt iſte factor $aa+bb$, hoc eſt vlla duorum quadratorum ſumma ſit diuiſibilis per $4n-1$. Q. E. D.

Coroll. 1.

17. Cum omnes numeri primi vel ad hanc formam $4n+1$ vel ad hanc $4n-1$ reuocentur, ſi $4n-1$ non fuerit numerus primus, diuiſorem habebit formae $4n-1$; namque ex meris numeris formae $4n+1$ nunquam numerus formae $4n-1$ reſultare poteſt. Quare cum ſumma duorum quadratorum per nullum numerum primum formae $4n-1$ diuidi poſſit, per nullum quoque numerum eiusdem formae $4n-1$, etiamſi non ſit primus dividi poterit.

Coroll. 2.

18. Summa ergo duorum quadratorum $aa+bb$, per nullum numerum huius ſeriei:

3, 7, 11, 15, 19, 23, 27, 31, 35, etc.

eſt diuiſibilis. Omnes ergo numeri primi praeter binarium, qui vnquam diuiſores eſſe poſſunt ſummae duorum quadratorum, continentur in hac forma $4n+1$; ſiquidem numeri $\underline{a}$ et $\underline{b}$ inter ſe communem diuiſorem non habent.

Coroll. 3.

19. Cum omnis numerus ſit vel primus vel productum ex primis, ſumma duorum quadratorum nullum numerum primum pro diuiſore habebit, niſi qui contineatur

tur in hac forma $4n+1$. Diuiſores ergo primi ſummae duorum quadratorum continebuntur in hac ſerie:
2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, etc.

Scholion.

20. Quod numerus huius formae $4n-1$ nunquam poſſit eſſe ſumma duorum quadratorum, facile intelligitur. Numeri enim quadrati vel ſunt pares vel impares, illi in hac forma $4a$, hi vero in hac $4b+1$ continentur. Quare vt ſumma duorum quadratorum ſit numerus impar, alterum par alterum impar eſſe oportet, hinc oritur forma $4a+4b+1$ ſeu $4n+1$, ideoque nullus numerus huius formae $4n-1$ ſumma duorum quadratorum eſſe poteſt. Quod vero ſumma duorum quadratorum ne diuiſorem quidem formae $4n-1$ admittat, ab omnibus ſcriptoribus methodi Diophanteae ſemper eſt affirmatum: nemo autem vnquam, quantum mihi conſtat, id demonſtrauit, excepto Fermatio, qui autem ſuam demonſtrationem nunquam publicauit, ita vt mihi quidem videar primus hanc veritatem publice demonſtraſſe; nullum numerum vel huius formae $4n-1$ vel per numerum eiusdem formae diuiſibilem vnquam eſſe poſſe ſummam duorum quadratorum. Hinc ergo ſequitur omnem ſummam duorum quadratorum inter ſe primorum vel eſſe numerum primum, vel binario excepto alios diuiſores non habere, niſi qui in forma $4n+1$ contineantur.

Theorema 6.

21. Omnes diuiſores ſummae duorum biquadratorum inter ſe primorum ſunt vel 2, vel numeri huius formae $8n+1$.

Demon-

Demonſtratio.

Sint a^4 et b^4 duo biquadrata inter ſe prima, erit vel vtrumque impar, vel alterum par et alterum impar; priori caſu ſummae a^4+b^4 diuiſor erit 2; vtroque vero caſu diuiſores impares, ſi qui fuerint, in hac forma $4n+1$ continebuntur. Cum enim biquadrata ſimul ſint quadrata, nullus diuiſor formae $4n-1$ locum invenit (16). At numeri $4n+1$ vel ad hanc formam $8n+1$ vel ad hanc $8n-3$ reuocantur. Dico autem nullum numerum formae $8n-3$ eſſe poſſe diuiſorem ſummae duorum biquadratorum. Ad hoc demonſtrandum ſit primo $8n-3$ numerus primus, atque per eum diuiſibilis erit haec forma $a^{8n-4}-b^{8n-4}$, vnde haec forma $a^{8n-4}+b^{8n-4}$ per numerum $8n-3$ prorſus non erit diuiſibilis, niſi vterque numerus a et b ſeorſim diuiſionem admittat, qui caſus autem aſſumtione, quod ambo numeri a et b ſint inter ſe primi excluditur. Cum igitur forma $a^{8n-4}+b^{8n-4}=a^{4(2n-1)}+b^{4(2n-1)}$ diuidi nequeat per $8n-3$, nullus quoque eius factor per $8n-3$ diuidi poterit. At ob $2n-1$ numerum imparem, illius formae factor erit a^4+b^4, qui ergo per nullum numerum primum formae $8n-3$ diuidi poteſt. Hinc omnes numeri primi praeter binarium, qui vnquam formam a^4+b^4 diuident, erunt huiusmodi $8n+1$. Ex multiplicatione autem duorum pluriumue talium diuiſorum nunquam numerus formae $8n-3$ oritur: ex quo ſequitur nullum prorſus numerum huius formae $8n-3$ ſiue ſit primus ſiue compoſitus, ſummam duorum biquadratorum inter ſe primorum diuidere. Q. E. D.

Coroll. 1.

22. Cum omnes numeri impares in vna harum quatuor formarum contineantur: $8n \pm 1$ et $8n \pm 3$: praeter numeros in forma prima $8n+1$ contentos nullus alius poterit esse diuisor summae duorum biquadratorum.

Coroll. 2.

23. Omnes ergo diuisores primi summae duorum biquadratorum inter se primorum erunt vel 2 vel in hac serie contenti. 17, 41, 73, 89, 97, 113, 137, 193, etc. quae complectitur omnes numeros primos formae $8n+1$.

Coroll. 3.

24. Si quis ergo numerus puta N fuerit summa duorum biquadratorum, tum is vel erit primus, vel alios non habebit diuisores, nisi qui in forma $8n+1$ contineantur; vnde inuestigatio diuisorum mirum in modum contrahitur.

Coroll. 4.

25. Nullus igitur numerus, qui diuisorem habet non in forma $8n+1$ contentum, erit summa duorum biquadratorum; nisi forte habeat quatuor diuisores aequales, qui autem in consideratione biquadratorum reiici solent.

Theorema 7.

26. Omnes diuisores huiusmodi numerorum a^8+b^8 si quidem a et b sunt numeri inter se primi, sunt vel 2 vel in hac forma $16n+1$ continentur.

Demon-

Demonſtratio.

Quia a^8 et b^8 ſimul ſunt biquadrata, eorum ſumma $a^8 + b^8$ alios non admittet diuiſores, niſi qui in forma $8n+1$ contineantur. At numeri in hac forma $8n+1$ contenti ſunt vel $16n+1$ vel $16n-7$. Sit $16n-7$ numerus primus, ac per eum diuidi non poterit forma $a^{16n-8}+b^{16n-8}$ (13). ſeu $a^{8(2n-1)}+b^{8(2n-1)}$, neque propterea vllus eius factor. Verum ob $2n-1$ numerum imparem haec forma diuiſorem habet a^8+b^8, quae ergo per nullum numerum primum $16n-7$ erit diuiſibilis, ac propterea alios diuiſores primos habere nequit, niſi qui in forma $16n+1$ contineantur. Ex multiplicatione autem duorum pluriumue huiusmodi numerorum $16n+1$, perpetuo productum eiusdem formae naſcitur, neque vnquam numerus formae $16n-7$ reſultare poteſt. Vnde cum nullus numerus formae $16n-7$ diviſor ipſius a^8+b^8 exiſtere poſſit, neceſſe eſt vt omnes huius formae a^8+b^8 diuiſores, ſi quos habet, ſiue ſint primi ſiue compoſiti, perpetuo in hac formula $16n+1$ contineantur. Q. E. D.

Coroll. 1.

27. Nullus igitur numerus, qui in hac forma $16n+1$ non includitur, vnquam eſſe poteſt diuiſor ſummae duarum poteſtatum octaui gradus inter ſe primarum.

Coroll. 2.

28 Si quis ergo voluerit numeri cuiuspiam huius formae a^8+b^8 diuiſores inueſtigare, is diuiſionem per nullos alios numeros primos niſi in hac forma $16n+1$

con-

contentos, tentet, cum demonſtratum ſit omnes reliquos numeros primos huius formae diuiſores eſſe non poſſe.

Theorema 8.

29. Summa duarum huiusmodi poteſtatum $a^{2^m}+b^{2^m}$ quarum exponens eſt dignitas binarii alios diuiſores non admittit, niſi qui contineantur in hac forma $2^{m+1}n+1$.

Demonſtratio.

Quemadmodum demonſtrauimus omnes diuiſores formae a^2+b^2 in hac forma $4n+1$ contineri, hincque vlterius diuiſores omnes formae a^4+b^4 in $8n+1$ et formae a^8+b^8 in $16n+1$ contineri euicimus; ita ſimili modo oſtendi poteſt formam $a^{16}+b^{16}$ nullos alios diuiſores admittere niſi in formula $32n+1$ contentos. Dehinc porro intelligemus formas $a^{32}+b^{32}$; $a^{64}+b^{64}$ etc. alios diuiſores habere non poſſe, niſi qui in formulis $64n+1$, $128n+1$ etc. includantur. Sicque in genere patebit formae $a^{2^m}+b^{2^m}$ alios non dari diuiſores, niſi qui in formula $2^{m+1}n+1$ contineantur. Q. E. D.

Coroll. 1.

30. Nullus ergo numerus primus, qui in hac forma $2^{m+1}n+1$ non includitur, vnquam eſſe poteſt diuiſor vllius numeri in hac forma $a^{2^m}+b^{2^m}$ contenti.

Coroll. 2.

31. Diuiſores ergo huiusmodi numeri $a^{2^m}+b^{2^m}$ inquiſiturus inutiliter operam ſuam comſumeret, ſi aliis numeris primis praeter eos, quas forma $2^{m+1}n+1$ ſuppeditat, diuiſionem tentare vellet.

Scholion

Scholion 1.

32. Fermatius affirmauerant, etiamsi id se demonstrare non posse ingenue esset confessus, omnes numeros ex hac forma $2^{2^m}+1$ ortos esse primos; hincque problema alias difficillimum, quo quaerebatur numerus primus dato numero maior, resoluere est conatus. Ex vltimo theoremate autem perspicuum est, nisi numerus $2^{2^m}+1$ sit primus eum alios diuisores habere non posse praeter tales, qui in forma $2^{m+1}n+1$ contineantur. Cum igitur veritatem huius effati Fermatiani pro casu $2^{32}+1$ examinare voluissem, ingens hinc compendium sum nactus, dum diuisionem aliis numeris primis, praeter eos, quos formula $64n+1$ suppeditat, tentare non opus habebam. Huc igitur inquisitione reducta mox deprehendi ponendo $n=10$ numerum primum 641 esse diuisorem numeri $2^{32}+1$, vnde problema memoratum, quo numerus primus dato numero maior requiritur, etiamnum manet insolutum.

Scholion 2.

33. Summa duarum potestatum eiusdem gradus vti a^m+b^m semper habet diuisores algebraice assignabiles, nisi m sit dignitas binarii. Nam si m sit numerus impar, tum a^m+b^m semper diuisorem habet $a+b$, atque si p fuerit diuisor ipsius m, tum quoque a^p+b^p formam a^m+b^m diuidet. Sin autem m sit numerus par, in hac formula $2^n p$ continebitur, ita vt p sit numerus impar, hocque casu $a^{2^n}+b^{2^n}$ diuisor erit formae a^m+b^m existente $m=2^n p$. Atque si p habeat diuisorem q, tum

etiam $a^{2^n q} + b^{2^n q}$ erit diuiſor formae $a^m + b^m$. Quocirca $a^m + b^m$ numerus primus eſſe nequit niſi m ſit dignitas binarii. Hoc igitur caſu, ſi $a^m + b^m$, non fuerit numerus primus, alios diuiſores habere nequit, niſi qui formula $2mn + 1$ contineantur. Contra autem ſi differentia duarum poteſtatum eiusdem gradus proponatur $a^m - b^m$, ea ſemper diuiſorem habet $a - b$; praeterea vero ſi exponens m diuiſorem habeat p, erit quoque $a^p - b^p$ diuiſor formae $a^m - b^m$. Hinc ſi m ſit numerus primus forma $a^m - b^m$ praeter $a - b$ alium diuiſorem algebraice aſſignabilem non habebit, quare ſi $a^m - b^m$ fuerit numerus primus, neceſſe eſt vt m ſit numerus primus et $a - b = 1$. Interim tamen ne his quidem caſibus forma $a^m - b^m$ ſemper eſt numerus primus; ſed quoties $2m + 1$ eſt numerus primus, per eum erit diuiſibilis. Praeterea vero etiam alios diuiſores habere poteſt, quos hic ſum inueſtigaturus.

Theorema 9.

34. Si differentia poteſtatum $a^m - b^m$ fuerit diuiſibilis per numerum primum $2n + 1$, atque p ſit maximus communis diuiſor numerorum m et $2n$, tum quoque $a^p - b^p$ erit diuiſibilis per $2n + 1$.

Demonſtratio.

Quia $2n + 1$ eſt numerus primus, erit $a^{2n} - b^{2n}$ diuiſibilis per $2n + 1$, et cum per hypotheſin $a^m - b^m$ ſit quoque diuiſibilis per $2n + 1$. Sit $2n = \alpha m + q$, ſeu q ſit reſiduum in diuiſione ipſius $2n$ per m remanens; et cum $a^{\alpha m} - b^{\alpha m}$ ſit quoque per $2n + 1$ diuiſibilis, multiplicetur haec forma per a^q, erit $a^{\alpha m + q} - a^q b^{\alpha m}$ per

2n

$2n+1$ diuisibilis: at posito $\alpha m+q$ pro $2n$ est quoque $a^{\alpha m+q}-b^{\alpha m+q}$ per $2n+1$ diuisibilis: a qua formula si prior subtrahatur, residuum $a^q b^{\alpha m}-b^{\alpha m+q}=b^{\alpha m}(a^q-b^q)$ quoque per $2n+1$ erit diuisibile. Hinc cum b per hypothesin diuisorem $2n+1$ non habeat, necesse est vt a^q-b^q per $2n+1$ sit diuisibile. Ponatur porro $m=\beta q+r$, et cum vtraque haec formula $a^{\beta q+r}-b^{\beta q+r}$ et $a^{\beta q}-b^{\beta q}$ sit per $2n+1$ diuisibilis, multiplicetur posterior per a^r et a priori subtrahatur, atque residuum $b^{\beta q}(a^r-b^r)$ seu a^r-b^r pariter per $2n+1$ erit diuisibile. Simili modo patebit, si fuerit $q=\gamma r+s$ tam formulam a^s-b^s per $2n+1$ fore diuisibilem; atque si per huiusmodi continuam diuisionem valores litterarum q, r, s, t etc. inuestigentur, tandem peruenietur ad maximum communem diuisorem numerorum m et $2n$, qui ergo si ponatur $=p$, erit a^p-b^p diuisibile per $2n+1$. Q. E. D.

Coroll. 1.

35. Si igitur m fuerit numerus ad $2n$ primus, maximus eorum communis diuisor erit vnitas, ac propterea si a^m-b^m fuerit diuisibile per numerum primum $2n+1$, tum quoque $a-b$ per $2n+1$ erit diuisibile.

Coroll. 2.

36. Si ergo differentia numerorum $a-b$ non fuerit diuisibilis per $2n+1$, tum quoque nulla huiusmodi forma a^m-b^m, vbi m est ad $2n$ numerus primus, per $2n+1$ diuisibilis esse potest.

Coroll. 1.

37. Quodsi ergo m fuerit numerus primus, forma

$a^m - b^m$ per numerum primum $2n+1$ diuidi non poteſt niſi m ſit diuiſor ipſius $2n$; poſito quod $a-b$ non ſit diuiſibile per $2n+1$.

Coroll. 4.

38. Exiſtente ergo m numero primo, haec forma $a^m - b^m$ praeter diuiſorem $a-b$ alios diuiſores habere nequit, niſi qui includantur in hac formula $mn+1$. Vnde diuiſores numeri cuiuspiam in hac forma $a^m - b^m$ contenti inueſtigaturus diuiſionem tantum per numeros primos in forma $mn+1$ contentos tentabit.

Coroll. 5.

39. Niſi ergo numerus $2^m - 1$ ſit primus, exiſtente m numero primo, alios diuiſores habere non poterit, niſi qui includantur in hac forma $mn+1$.

Coroll. 6.

40. Si ergo m ſit numerus primus, diuiſores formulae $a^m - b^m$ praeter $a-b$, ſi quidem a et b fuerint numeri inter ſe primi, continebuntur in hac ſerie: $2m+1$; $4m+1$; $6m+1$; $8m+1$; $10m+1$; etc. ſi hinc numeri non primi expungantur.

Theorema 10.

41. Si formula $a^m + b^m$ diuiſorem habeat p, tum quoque haec expreſſio $(a \pm \alpha p)^m \pm (b \pm \beta p)^m$ per p erit diuiſibilis.

Demonſtratio.

Si poteſtates $(a \pm \alpha p)^m$ et $(b \pm \beta p)^m$ methodo conſueta euoluantur, in vtraque ſerie omnes termini prae-

ter

ter primum diuiſibiles erunt per p. Scilicet formula $(a \pm \alpha p)^m \pm (b \pm \beta p)^m$ abibit in hanc formam:

$$\mp a^m \pm m a^{m-1} \alpha p + \frac{m(m-1)}{1 \cdot 2} a^{m-2} \alpha^2 p^2 \pm \text{etc.}$$

$$\pm (b^m \pm m b^{m-1} \beta p - \frac{m(m-1)}{1 \cdot 2} b^{m-2} \beta^2 p^2 \pm \text{etc.})$$

Vnde perſpicuum eſt ſi $a^m - b^m$ fuerit diuiſibile, tum quoque haec forma $(a \pm \alpha p)^m - (b \pm \beta p)^m$ per p erit diuiſibilis. Q. E. D.

Coroll. 1.

42. Si igitur $a^m \pm 1$ fuerit diuiſibile per p, tum quoque haec formula $(a \pm \alpha p)^m \pm 1$ per p erit diuiſibilis.

Coroll. 2.

43. Si $a^m \pm b^m$ fuerit diuiſibile per p, tum quoque haec formula $(a \pm \alpha p)^m \pm b^m$, vel haec $a^m \pm (b \pm \beta p)^m$ per p erit diuiſibilis.

Scholion.

44. Eodem quoque modo generaliter demonſtrari poteſt, ſi fuerit $A a^m \pm B b^m$ diuiſibile per p, tum quoque hanc formam $A(a \pm \alpha p)^m \pm B(b \pm \beta p)^m$ fore per p diuiſibilem. Haecque veritas aeque locum inuenit, ſiue p ſit numerus primus ſiue ſecus. Quin etiam non opus eſt, vt vtriusque poteſtatis idem ſit exponens m, ſed etiamſi eſſent inaequales, concluſio perinde valebit. Tum vero quoque ſi m fuerit numerus par ex diuiſibilitate formulae $a^m \pm b^m$ per numerum p, diuiſibilitas etiam huius formulae $(\alpha p \pm a)^m \pm (\beta p \pm b)^m$ ſequitur. Verum haec aliaque ſimilia ex algebrae elementis ſponte patent.

Theorema 11.

45. Si fuerit $a = ff \pm (2m+1)\alpha$, et $2m+1$ numerus primus, tum ista expressio $a^m - 1$ erit diuisibilis per $2m+1$.

Demonstratio.

Cum sit $2m+1$ numerus primus, per eum diuidi poterit haec formula $f^{2m} - 1$, seu haec $(ff)^m - 1$. Hinc per theorema praecedens quoque ista formula $(ff \pm (2m+1)\alpha)^m - 1$ erit diuisibilis per $2m+1$. Quare si fuerit $a = ff \pm (2m+1)\alpha$, formula $a^m - 1$ per numerum primum $2m+1$ diuidi poterit. Q. E. D.

Coroll. 1.

46. Si ergo fuerit vel $a = (2m+1)\alpha + 1$ vel $a = (2m+1)\alpha + 4$, vel $a = (2m+1)\alpha + 9$; vel $a = (2m+1)\alpha + 16$ vel etc. tum formula $a^m - 1$ semper erit diuisibilis per $2m+1$, si quidem $2m+1$ fuerit numerus primus.

Coroll. 2.

46. Cum casus, quibus ipse numerus a est diuisibilis per $2m+1$ excludantur, manifestum est in formula $ff \pm (2m+1)\alpha$ numerum f per $2m+1$ diuisibilem esse non posse. Hinc pro f omnes numeri assumi possunt qui per $2m+1$ non sint diuisibiles.

Coroll. 3.

47. Numeri ergo pro f assumendi sunt $(2m+1)k \pm 1$; $(2m+1)k \pm 2$; $(2m+1)k \pm 3$; .... $(2m+1)k \pm m$: in his enim formulis omnes numeri per $2m+1$ non diuisibiles continentur. Hinc sumendis quadratis

dratis formae ipsius a, si quidem partes per $2m+1$ diuisibiles in vnum colligantur, erunt sequentes: $(2m+1)p+1$; $(2m+1)p+4$; $(2m+1)p+q$; .... $(2m+1)p+mm$ quarum numerus est m.

Coroll. 4.

48. Ad valores igitur ipsius a inueniendos, vt a^m-1 per numerum primum $2m+1$ fiat diuisibile, inuestigari oportet residua, quae in diuisione cuiusque numeri quadrati per $2m+1$ remanent. Si enim r fuerit huius modi residuum, erit $(2m+1)p+r$ idoneus valor pro a.

Coroll. 5.

49. Omnia haec residua r erunt autem minora quam $2m+1$, neque tamen omnes numeri minores quam $2m+1$ erunt valores ipsius r; quia numerus valorum ipsius r maior esse nequit quam m. Dabuntur ergo semper m numeri, qui pro r adhiberi non poterunt.

Coroll. 6.

50. Valores vero ipsius r erunt primo omnes numeri quadrati ipso $2m+1$ minores, tum vero residua, quae in diuisione maiorum quadratorum per $2m+1$ remanent, neque tamen vnquam numerus omnium diuersorum valorum ipsius r. maior esse poterit numero m.

Scholion.

51. Vt vsus huius theorematis clarius appareat, atque per exempla numerica illustrari possit, sequentia problemata adiicere visum est, ex quibus non solum veritas theorematis luculentius perspicietur, sed etiam vicissim patebit

tebit, quoties a non habuerit valorem hic assignatum, toties formulam $a^m - 1$ non esse diuisibilem per $2m+1$. Cum igitur haec formula $a^{2m} - 1$ semper sit diuisibilis per $2m+1$, quoties $a^m - 1$ diuisionem per $2m+1$ non admittit, toties $a^m + 1$ per $2m+1$ diuisibile esse oportebit.

Exempl. 1.

52. *Inuenire valores ipsius* a, *vt* $a^2 - 1$ *fiat diuisibile per* 5.

Residua, quae ex diuisione quadratorum per 5 remanent sunt 1 et 4; hinc necesse est vt sit vel $a = 5p+1$ vel $a = 5p+4$, siue $a = 5p+1$. Priori casu fit $aa - 1$ seu $(a-1)(a+1) = 5p(5p+2)$ posteriori autem $= (5p-2)5p$. vtroque ergo diuisibilitas per 5 perspicitur. Sin autem fuerit vel $a = 5p+2$, vel vel $a = 5p+3$ neutro casu formula $aa - 1$ per 5 erit diuisibilis.

Exempl. 2.

53. *Inuenire valores ipsius* a, *vt haec forma* $a^3 - 1$ *fiat per* 7 *diuisibilis.*

Tria residua, quae in diuisione omnium quadratorum per 7 remanent sunt, 1, 2, 4. Hinc valores ipsius a sunt: $7p+1$; $7p+2$, et $7p+4$, sin autem fuerit vel $a = 7p+3$ vel $7p+5$ vel $7p+6$, tum non formula proposita $a^3 - 1$ sed haec $a^3 + 1$ per 7 fiet diuisibilis.

Exempl. 3.

54. *Inuenire valores ipsius* a *vt haec forma* $a^5 - 1$ *fiat per* 11 *diuisibilis.*

Nu-

Numeri quadrati per 11 diuifi dabunt 5 diuerfa refidua quae funt: 1, 3, 4, 5, 9. Hinc formula $a^5 - 1$ per 11 erit diuifibilis, fi fuerit $a = 11p + r$ denotante r vnumquemque ex numeris 1, 3, 4, 5, 9. Sin autem pro a fumatur quidam ex his numeris 2, 6, 7, 8, 10 multiplo quocunque ipfius 11 auctus, tum $a^5 + 1$ per 11 erit diuifibile.

Theorema 12.

55. Si fuerit $a = f^3 \pm (3m+1)\alpha$, exiftente $3m+1$ numero primo, tum haec forma $a^m - 1$ femper erit per $3m+1$ diuifibilis.

Demonftratio.

Ob $3m+1$ numerum primum erit $f^{3m} - 1$ divifibile per $3m+1$. At eft $f^{3m} - 1 = (f^3)^m - 1$, vnde quoque haec formula $(f^3 \pm (3m+1)\alpha)^m - 1$ erit diuifibilis per $3m+1$. Quare fi fumatur $a = f^3 \pm (3m+1)\alpha$, tum haec formula $a^m - 1$ erit per $3m+1$ diuifibilis. Q. E. D.

Coroll. 1.

56. Ad valores ergo ipfius a inueniendos, omnia refidua quae oriuntur, fi cubi per $3m+1$ diuidantur, notari debent. Vnumquodque enim horum refiduorum multiplo ipfius $3m+1$ quocunque auctum dabit valorem idoneum pro a.

Coroll. 2.

57. Cum $3m+1$ effe debeat numerus primus, neceffe eft vt m fit numerus par, ficque numerus primus $3m+1$ vnitate fuperabit multiplum fenarii. Hinc erunt numeri pro m et $3m+1$ adhibendi fequentes:

m	2, 4, 6, 10, 12, 14, 20, 22, 24, 26, 32 etc.
$3m+1$;	7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, etc.

Coroll. 3.

58. Si ergo numeri cubici per hos numeros primos $3m+1$ diuidantur, sequentia residua remanebunt:

Diuisores	Residua
7	1, 6
13	1, 5, 8, 12
19	1, 7, 8, 11, 12, 18
31	1, 2, 4, 8, 15, 16, 23, 27, 29, 30
37	1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36
	etc.

In his residuis primo occurrunt omnes cubi diuisoribus minores, deinde si quodpiam residuum fuerit r pro diuisore $3m+1$, tum quoque aliud dabitur residuum $=3m+1-r$. si enim cubus f^3 dederit residuum r, cubus $(3m+1-f)^3$ dabit residuum $-r$ seu $3m+1-r$.

Scholion.

59. Notatu hic dignum est numerum residuorum perpetuo esse $=m$, si diuisor fuerit $=3m+1$. Semper ergo dantur tres cubi, quorum radices sint $< 3m+1$, ex quibus idem residuum resultat. Scilicet hi tres cubi 1^3, 2^3, 4^3 per 7 diuisi idem dant residuum $=1$, et hi tres cubi 2^3, 5^3, et 6^3 per 13 diuisi idem dant residuum 8. Praeterea hic notari conuenit, si pro a alii valores praeter hos assignatos capiantur, tum a^m-1 non esse per $3m+1$ diuisibile, quod etsi verum esse facile depre-

prehenditur, tamen eius demonſtratio ex praecedentibus non ſequitur, pertinetque haec veritas ad id genus, quod nobis noſſe, non autem demonſtrare licet. His ergo caſibus, quibus $a^m - 1$ per $3m+1$ non eſt diuiſibile, haec formula $a^{2m}+a^m+1$ diuiſionem admittet.

Theorema 13.

60. Si fuerit $a = f^n \pm (mn+1)\alpha$ exiſtente $mn+1$ numero primo, tum haec forma $a^m - 1$ erit diuiſibilis per $mn+1$.

Demonſtratio.

Ob $mn+1$ numerum primum erit $f^{mn}-1$ diuiſibile per $mn+1$. At eſt $f^{mn}-1 = (f^n)^m - 1$, vnde quoque haec forma $(f^n \pm (mn+1)\alpha)^m - 1$ erit diuiſibilis per $mn+1$. Quare ſi ponatur $a = f^n \pm (mn+1)\alpha$, haec formula $a^m - 1$ per $mn+1$ diuidi poterit. Q. E. D.

Coroll. 1.

61. Si ergo poteſtates exponentis n per numerum primum $mn+1$ diuidantur, ſingula reſidua vel ipſa vel multiplo ipſius $mn+1$ quocunque aucta idoneos praebebunt valores pro a, vt $a^m - 1$ fiat per $mn+1$ diuiſibile.

Coroll. 2.

62. Hinc ſi $a^m - 1$ non fuerit per $mn+1$ diuiſibile, tum valor ipſius a in hac expreſſione $f^n \pm (mn+1)\alpha$ non continebitur, ſeu nulla dabitur poteſtas exponentis n quae per $mn+1$ diuiſa relinquat a.

Scholion.

63. Propositionis huius conuersa, si omni modo examinetur, quoque vera deprehenditur; ita vt quoties $a^m - 1$ sit diuisibile per $mn + 1$. toties quoque valor ipsius a in formula $f^n \pm (mn + 1)\alpha$ contineatur; seu toties dabitur potestas f^n quae per $mn + 1$ diuisa relinquat a pro residuo. Ita cum obseruassem formulam $2^{64} - 1$ esse per 641 diuisibilem, ob $m = 64$ fiet $n = 10$, dabitur quoque potestas dignitatis decimae, quae per 641 diuisa relinquat 2. Atque reuera huiusmodi potestatem deprehendi esse 96^{10}. Praeterea vero cum $2^{32} - 1$ non sit diuisibile per 641, hoc casu fit $m = 32$ et $n = 20$; nulla igitur datur potestas dignitatis vicesimae, quae per 641 diuisa relinquat 2. Veritas huius posterioris afferti rigorose est euicta, sed adhuc desideratur demonstratio harum propositionum conuersarum: scilicet si $a^m - 1$ fuerit diuisibile per numerum primum $mn + 1$, tum quoque semper a esse numerum in hac formula $f^n \pm (mn + 1)\alpha$ comprehensum. Atque si a non contineatur in formula $f^n \pm (mn + 1)\alpha$ tum quoque $a^m - 1$ per $mn + 1$ diuisionem non admittere. Quarum propositionum si altera demonstrari posset, simul veritas alterius esset euicta. Ceterum theorema hic demonstratum huc redit, vt quoties $f^n - a$ fuerit diuisibile per $mn + 1$, toties quoque formula $a^m - 1$ sit per $mn + 1$ diuisibilis. In hoc genere latius patet theorema sequens.

Theorema 14.

64. Si fuerit $f^n - ag^n$ diuisibile per numerum primum $mn + 1$, tum quoque $a^m - 1$ erit diuisibile per $mn + 1$.

De-

Demonstratio.

Cum ponatur formula $f^n - ag^n$ diuisibilis per $mn + 1$, erit quoque haec formula $f^{mn} - a^m g^{mn}$, quippe quae per illam diuidi potest, diuisibilis per $mn + 1$. At cum $mn + 1$ sit numerus primus, per eum diuisibilis erit haec forma $f^{mn} - g^{mn}$; vnde quoque differentia $g^{mn}(a^m - 1)$ seu ipsa formula $a^m - 1$ per $mn + 1$ erit diuisibilis, propterea quod g per $mn + 1$ diuisionem admittere nequeat, nisi simul f per eundem esset diuisibile, qui casus in nostro ratiocinio perpetuo excluditur. Q. E. D.

Coroll. 1.

65. Si ergo $a^m - 1$ per $mn + 1$ non fuerit diuisibile, tum quoque nulli dantur numeri f et g vt haec formula $f^n - ag^n$ per $mn + 1$ fiat diuisibilis.

Coroll. 2.

66. Si superioris propositionis conuersa demonstrari posset, tum quoque euictum foret: quoties $f^n - a$ per $mn + 1$ diuidi nequeat, tum ne hanc quidem formulam $f^n - ag^n$ diuisionem per $mn + 1$ admittere posse, simul vero etiam pateret, si $f^n - ag^n$ sit diuisibile per $mn + 1$, tum quoque dari huiusmodi formulam $f^n - a$, quae sit per $mn + 1$ diuisibilis.

Theorema 15.

67. Si huiusmodi formula $af^n - bg^n$ fuerit diuisibilis per numerum primum $mn + 1$, tum quoque haec formula $a^m - b^m$ erit per $mn + 1$ diuisibilis.

Demonſtratio.

Si fuerit $af^n - bg^n$ diuiſibile per $mn+1$, tum quoque haec formula $a^m f^{mn} - b^m g^{mn}$ erit per $mn+1$ diuiſibilis. At ob $mn+1$ numerum primum erit quoque haec formula $f^{mn} - g^{mn}$, ideoque et haec $a^m f^{mn} - a^m g^{mn}$ per $mn+1$ diuiſibilis, ſubtrahatur haec ab illa $a^m f^{mn} - b^m g^{mn}$ atque reſiduum $g^{mn}(a^m - b^m)$ ſeu $a^m - b^m$ per $mn+1$ erit diuiſibile. Q. E. D.

Coroll. 1.

68. Si itaque $a^m - b^m$ non fuerit per $mn+1$ diviſibile, tum nulli dabuntur numeri pro f et g ſubſtituendi, vt huiusmodi formula $af^n - bg^n$ ſit per $mn+1$ diuiſibilis.

Coroll. 2.

69. Huius propoſitionis conuerſa, quod, ſi fuerit formula $a^m - b^m$ diuiſibilis per $mn+1$, ſimul dentur numeri f et g, vt $af^n - bg^n$ fiat diuiſibilis per $mn+1$ vtcunque examinetur, vera deprehenditur. Interim tamen eius demonſtratio etiamnum deſideratur.

Scholion.

70. Caſus huius propoſitionis inuerſae demonſtrari poteſt, quo numeri m et n ſunt inter ſe primi: hoc enim caſu ſemper eiusmodi numeri μ et ν exhiberi poſſunt, vt ſit $\mu n \pm 1 = \nu m$. Namque ſi inter numeros m et n ea operatio inſtituatur, quae pro maximo communi diviſore inſtitui ſolet, atque quoti notentur, ex iiſque fractiones ad $\frac{m}{n}$ appropinquantes quaerantur, vltima erit $\frac{m}{n}$, et ſi penultima fuerit $\frac{\mu}{\nu}$ erit $\mu n \pm 1 = \nu m$. Hoc ergo lem-

lemmate praemisso demonstratio propositionis conuersae, qua m et n sunt numeri inter se primi ita se habebit.

Theorema 16.

71. Si m et n fuerint numeri primi inter se, atque ista formula $a^m - b^m$ diuisibilis sit per numerum $mn + 1$, tum dabitur formula $af^n - bg^n$ diuisibilis per $mn + 1$.

Demonstratio.

Ponatur $f = a^\mu$ et $g = b^\mu$, atque formula $af^n - bg^n$ abibit in hanc $a^{\mu n + 1} - b^{\mu n + 1}$, quare si μ ita capiatur, vt sit $\mu n + 1 = \nu m$, habebitur $a^{\nu m} - b^{\nu m}$, quae cum sit diuisibis per $a^m - b^m$, quoque per $mn + 1$ diuisibilis erit, sicque dabitur casus, quo $af^n - bg^n$ diuisibile erit per $mn + 1$. Sin autem fuerit $\mu n - 1 = \nu m$, tum sumatur $f = b^\mu$ et $g = a^\mu$ fietque $af^n - bg^n = ab^{\mu n} - ba^{\mu n} = ab(b^{\mu n - 1} - a^{\mu n - 1}) = -ab(a^{\nu m} - b^{\nu m})$ ideoque erit per $mn + 1$ diuisibilis. Q. E. D.

Coroll. 1.

72. Si ergo m et n fuerint numeri inter se primi, atque $mn + 1$ numerus primus, tum istae propositiones sunt demonstratae. I. Si $af^n - bg^n$ fuerit diuisibile per $mn + 1$, tum quoque $a^m - b^m$ erit per $mn + 1$ diuisibile, et si illa formula nullo modo sit diuisibilis per $mn + 1$, tum etiam haec non erit diuisibilis. II. Si $a^m - b^m$ fuerit diuisibile per $mn + 1$, tum dabitur numerus huius formae $af^n - bg^n$ per $mn + 1$ diuisibilis, atque si $a^m - b^m$ per $mn + 1$ diuisionem non admittat, tum nullus dabitur numerus formae $af^n - bg^n$ per $mn + 1$ diuisibilis.

Coroll.

Coroll. 2.

73. Si m ſit numerus par, tum b aeque negatiue atque affirmatiue accipi poteſt, hoc ergo caſu ſi $a^m - b^m$ fuerit diuiſibile per $mn + 1$, tum etiam eiusmodi formula $af^n + bg^n$ per $mn + 1$ diuiſibilis aſſignari poterit; id quod etiam inde patet, quod n ſit numerus impar, ideoque poteſtas g^n negatiua fieri queat.

Coroll. 3.

74. Simili modo demonſtrabitur, ſi fuerint vt ante m et n numeri inter ſe primi, atque haec formula $a^m - b^m$ ſit diuiſibilis per $mp + 1$, tum quoque exhiberi poſſe formulam huiusmodi $af^n - bg^n$ diuiſibilem per $mp + 1$.

VARIAE