



1750

Theoremata circa divisores numerorum

Leonhard Euler

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

 Part of the [Mathematics Commons](#)

Record Created:

2018-09-25

Recommended Citation

Euler, Leonhard, "Theoremata circa divisores numerorum" (1750). *Euler Archive - All Works*. 134.
<https://scholarlycommons.pacific.edu/euler-works/134>

This Article is brought to you for free and open access by the Euler Archive at Scholarly Commons. It has been accepted for inclusion in Euler Archive - All Works by an authorized administrator of Scholarly Commons. For more information, please contact mgibney@pacific.edu.

THEOREMATA

CIRCA DIVISORES NUMERORVM.

AVCTORE
L. EVLERO.

Quous tempore summi Geometrae agnouerunt in natura numerorum plurimas praeclarissimas proprietates esse absconditas, quarum cognitio fines matheos non mediocriter esset amplificatura. Primo quidem intuitu doctrina numerorum ad arithmeticae elementa referenda videtur, atque vix quicquam in ea inesse putatur, quod ullam 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 mathefi 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 matheos partibus maxime pertractata ac perspecta haberi solet: neque facile affirmare ausim, an similes veritates in reliquis partibus reperiantur. In Geometria certe nulla occurrit 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; ac 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 quaequam 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 patefacere solet. Hanc obrem non inuulter me operam ac studium in indagatione demonstrationum quarundam 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 $a^n + b^n$ 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 confitero euoluatur, erit $(a+b)^p = a^p + \frac{p}{1} a^{p-1} b + \frac{p(p-1)}{1 \cdot 2} a^{p-2} b^2 + \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3} a^{p-3} b^3 + \dots + \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3} a^3 b^{p-3} + \frac{p(p-1)}{1 \cdot 2} a^2 b^{p-2} + \frac{p}{1} a b^{p-1} + b^p$. qua expressioe substituta, binisque terminis, qui easdem habent uncias; coniunctis, erit $(a+b)^p - a^p - b^p = \frac{p}{1} ab(a^{p-2} + b^{p-2}) + \frac{p(p-1)}{1 \cdot 2} a^2 b^2 (a^{p-4} + b^{p-4}) + \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3} a^3 b^3 (a^{p-6} + b^{p-6}) + \frac{p(p-1)(p-2)(p-3)}{1 \cdot 2 \cdot 3 \cdot 4} (a^{p-8} + b^{p-8}) a^4 b^4 + \text{etc.}$ Hic primo notandum est omnes uncias, quamquam sub forma fractionum apparent, nihilominus esse numeros integros, cum exhibeant, vti constat numeros figuratos. Quaelibet ergo uncia 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 ultra $\frac{1}{2}p$ crescunt, ideoque factor numeratorum p nusquam per diuisionem tollitur. Deinde cum p sit per hypoth. numerus primus, is nusquam per diuisionem minuetur. Quocirca singulae unciae $\frac{p}{1}$; $\frac{p(p-1)}{1 \cdot 2}$; $\frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3}$; 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 fit $2^p-2=2(2^{p-1}-1)$: alterum horum factorum per p diuisibilem esse oportet. At nisi fit $p=2$, prior factor 2 per p non est diuisibilis: unde 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 aequae 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 assumpta 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. Quicumque 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 diuisibilis 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 , siquidem neque a neque b seorsim fuerit per $2m + 1$ diuisibilis.

Coroll. 2.

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

Tom. I.

D

 b^{2m}

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 $2m+1$, prædabit 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 diuisibile 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 $4n-1$ (II), hincque ista formula $a^{4n-2}+b^{4n-2}$ non erit diuisi-

diuisibilis per $4n-1$, neque propterea vllus eius factor. At cum $4n-2=2(2n-1)$ fit 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 fit 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 diuidi 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 a et 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 Diophantaeae 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 assumptione, 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 pluriusue 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: $8n + 1$ et $8n + 3$: 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 reijci solent.

Theorema 7.

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

Demon.

Demonstratio.

Quia a^2 et b^2 simul sunt biquadrata, eorum summa $a^2 + b^2$ alios non admittet diuifores, 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 ullus eius factor. Verum ob $2n - 1$ numerum imparem haec forma diuiforem habet $a^2 + b^2$, quae ergo per nullum numerum primum $16n - 7$ erit diuifibilis, ac propterea alios diuifores 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 $16n - 7$ diuifor ipfius $a^2 + b^2$ existere possit, necesse est vt omnes huius formae $a^2 + b^2$ diuifores, 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 diuifor summae duarum potestatum octauae gradus inter se primarum.

Coroll. 2.

28. Si quis ergo voluerit numeri cuiuspiam huius formae $a^2 + b^2$ diuifores inuestigare, is diuifionem 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 demonstrauius omnes diuisores formae $a^2 + b^2$ in hac forma $4n + 1$ contineri, hincque ulterius 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 consumeret, si aliis numeris primis praeter eos, quas forma $2^{m+1}n + 1$ supeditat, 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, resolvere est conatus. Ex ultimo theoremate autem perspicuum est, nisi numerus $2^{2^m} + 1$ sit primus eum alios diuifores 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 diuiforem 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 diuifores algebraice assignabiles, nisi m sit dignitas binarii. Nam si m sit numerus impar, tum $a^m + b^m$ semper diuiforem habet $a + b$, atque si p fuerit diuifor 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 $a^{2^n} + b^{2^n}$ diuifor erit formae $a^m + b^m$ existente $m = 2^n p$. Atque si p habeat diuiforem q , tum

Tom. I.

E

etiam

etiam $a^{2n}q + b^{2n}q$ erit diuisor formae $a^m + b^m$. Quo-
circa $a^m + b^m$ numerus primus esse nequit nisi m sit
dignitas binarii. Hoc igitur casu, si $a^m + b^m$, non fu-
erit 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 ve-
ro 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 af-
signabilem 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 nume-
rus 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 diuifi-
bilis per numerum primum $2n + 1$, atque p sit maxi-
mus 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 $m = \xi q + r$, et cum vtraque haec formula $a^{\xi q + r} - b^{\xi q + r}$ et $a^{\xi q} - b^{\xi q}$ sit per $2n+1$ diuisibilis, multiplicetur posterior per a^r et a priori subtrahatur, atque residuum $b^{\xi q} (a^r - b^r)$ 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

E 2

 a^m

$a^m - b^m$ per numerum primum $2n + 1$ diuidi non potest nisi m fit diuisor ipsius $2n$; positò 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 $mn + 1$. Unde 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 fit 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 $(a + ap)^m + (b + bp)^m$ per p erit diuisibilis.

Demonstratio.

Si potestates $(a + ap)^m$ et $(b + bp)^m$ methodo consueta euoluantur, in vtraque serie omnes termini praeter

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

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

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

Vnde perspicuum est si $a^m - b^m$ fuerit diuisibile, tum quoque haec forma $(a \pm \alpha p)^m - (b \pm \xi p)^m$ 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 $a^m \pm (b \pm \xi p)^m$ 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 $A(a \pm \alpha p)^m \pm B(b \pm \xi p)^m$ fore per p diuisibilem. Haecque veritas aequae locum inuenit, siue p sit numerus primus siue secus. Quin etiam non opus est, vt vtriusque potestatis idem sit exponens m , sed etiam si 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 $(\alpha p \pm a)^m \pm (\xi p \pm b)^m$ sequitur. Verum haec aliaque similia ex algebrae elementis sponte patent.

Theorema II.

45. Si fuerit $a = ff + (2m + 1)\alpha$, 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 $(ff + (2m + 1)\alpha)^m - 1$ erit diuisibilis per $2m + 1$. Quare si fuerit $a = ff + (2m + 1)\alpha$, formula $a^m - 1$ per numerum primum $2m + 1$ diuidi poterit. Q. E. D.

Coroll. I.

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 $ff + (2m + 1)\alpha$ 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 $(2m + 1)k + 1$; $(2m + 1)k + 2$; $(2m + 1)k + 3$; $(2m + 1)k + m$: 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 , ut $a^2 - 1$ fiat diuisibile per 5.

Residua, quae ex diuisione quadratorum per 5 remanent sunt 1 et 4; hinc necesse est ut 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 $= (5p - 2)5p$. utroque 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 , ut 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 ut haec forma $a^3 - 1$ fiat per 11 diuisibilis.

Numeri quadrati per 11 diuifi dabunt 5 diuerfa re-
 fidua quae sunt: 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
 quocunq̄ue ipfius 11 auctus, tum a^5+1 per 11 erit diuifibile.

Theorema 12.

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

Demonstratio.

Ob $3m+1$ numerum primum erit $f^{3m}-1$ di-
 uifibile per $3m+1$. At est $f^{3m}-1=(f^3)^m-1$, vnde
 quoque haec formula $(f^s+(3m+1)\alpha)^m-1$ erit diuifi-
 bilis per $3m+1$. Quare fi fumatur $a=f^s+(3m+1)\alpha$,
 tum haec formula a^m-1 erit per $3m+1$ diuifibi-
 lis. 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 $3m+1$ quocunq̄ue auctum dabit valorem
 idoneum pro a .

Coroll. 2.

57. Cum $3m+1$ effe debeat numerus primus,
 necesse est vt m fit numerus par, ficque numerus pri-
 mus $3m+1$ vnitare superabit multiplicam fenarii. Hinc
 erunt numeri pro m et $3m+1$ adhibendi fequentes:

Tom. I.

F

m

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 $a = f^n + (mn + 1)\alpha$ 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 $(f^n + (mn + 1)\alpha)^m - 1$ erit diuisibilis per $mn + 1$. Quare si ponatur $a = f^n + (mn + 1)\alpha$, 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 praebunt 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 $f^n + (mn + 1)\alpha$ 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 $a^m - 1$ fit 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 obseruarem 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 asserti 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 $f^{mn} - g^{mn}$; unde 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 effret 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 possit, 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 fit 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 $mn + 1$ diuisibile, tum nulli dabuntur numeri pro f et g substituendi, vt huiusmodi formula $af^n - bg^n$ fit 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 $\mu n + 1 = \nu m$. Namque si inter numeros m et n ea operatio instituat, quae pro maximo communi diuisore 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 $\mu n + 1 = \nu m$. Hoc ergo lem-

lemmate praemisso demonstratio propositionis conuerfae, 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 $a f^n - b g^n$ diuisibilis per $mn + 1$.

Demonstratio.

Ponatur $f = a^\mu$ et $g = b^\mu$, atque formula $a f^n - b g^n$ abibit in hanc $a^{\mu n + 1} - b^{\mu n + 1}$, quare si μ ita capiatur, ut sit $\mu n + 1 = \nu m$, habebitur $a^{\nu m} - b^{\nu m}$, quae cum sit diuisibilis per $a^m - b^m$, quoque per $mn + 1$ diuisibilis erit, sicque dabitur casus, quo $a j^n - b g^n$ diuisibile erit per $mn + 1$. Sin autem fuerit $\mu n - 1 = \nu m$, tum sumatur $f = b^\mu$ et $g = a^\mu$ fietque $a j^n - b g^n = a b^{\mu n} - b a^{\mu n} = a b (b^{\mu n - 1} - a^{\mu n - 1}) = -a b (a^{\nu m} - b^{\nu m})$ 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 $a j^n - b g^n$ 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 $a j^n - b g^n$ per $mn + 1$ diuisibilis, atque si $a^m - b^m$ per $mn + 1$ diuisiorem non admittat, tum nullus dabitur numerus formae $a j^n - b g^n$ per $mn + 1$ diuisibilis.

Coroll.

Coroll. 2.

73. Si m fit 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 fit numerus impar, ideoque potestas g^n negatiua fieri queat.

Coroll. 3.

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