



1761

Theoremata circa residua ex divisione potestatum relictata

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 residua ex divisione potestatum relictata" (1761). *Euler Archive - All Works*. 262.
<https://scholarlycommons.pacific.edu/euler-works/262>

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.



T H E O R E M A T A
CIRCA RESIDVA EX DIVISIONE
POTESTATVM RELICTA.

Auctore

L. EULERO.

Theorema. I.

I.

Si p fit numerus primus, et a primus ad p , nullus terminus huius progressionis geometricae $1, a, a^2, a^3, a^4, a^5, a^6$, etc. per numerum p diuisibilis existit.

Demonstratio.

Patet ex Euclidis Libro VII. Prop. 26. vbi demonstratur, si sint duo numeri a et b primi ad p , fore quoque productum ab primum ad p ; ideoque cum a fit primus ad p , erit posito $b = a$; quadratum a^2 primus ad p ; hincque porro a^3 posito $b = a^2$; item a^4 posito $b = a^3$; etc. Sic igitur nulla potestas ipsius a diuisibilis erit per numerum primum p .

Coroll. I.

2. Si igitur singuli termini progressionis geometricae

$1; a; a^2; a^3; a^4; a^5; a^6; a^7; a^8$; etc.

Tom. VII. Nou. Com.

G

per

per numerum primum p diuidantur, diuisio nunquam sine residuo succedet, sed ex singulis terminis orientur residua.

Scholion.

3. Residua haec, quae ex diuisione singulorum terminorum progressionis propositae geometricae per numerum primum p emergunt, hic diligentius perpendere constitui. Ac primo quidem singula haec residua, vti ex natura diuisionis apparet, minora erunt numero p ; nullum autem residuum erit $= 0$, quia nullus terminus per p est diuisibilis. Quodsi forte prodeant residua ipso numero p maiora, ex arithmetica constat, quemadmodum ea ad minora reduci oporteat. Sic residuum $p + r$ aequiualeat residuo r , et in genere residuum $np + r$ redit ad residuum r ; ac si r sit maius quam p , hoc residuum reuocatur ad $r - p$, vel $r - 2p$, vel $r - 3p$, etc. donec ad numerum ipso p minorem perueniatur. Itaque omnia haec residua $r + np$ pro eodem residuo r reputantur. Proprie autem loquendo omnia residua sunt numeri positiui ipso diuisore p minores. Verum tamen etiam saepenumero conuenit et residua negatiua contemplari: veluti si r sit residuum ex diuisione cuiuspiam numeri per p relictum, ita vt sit $r < p$, residuum quoque erit $r - p$, numerus scilicet negatiuus; ita vt residuum positiuum r aequiualeat residuo negatiuo $r - p$. Hoc modo residua ita exhiberi poterunt, vt nunquam semissem diuisoris p excedant; nam si residuum affirmatiuum r maius fuerit quam $\frac{1}{2}p$, eius loco capiatur residuum negatiuum $r - p$, quod minus erit, quam semissis ipsius p .

Coroll.

Coroll. 2.

4. Quoniam omnia residua sunt numeri integri, iique minores quam p ; sequitur plura diuersa residua oriri non posse quam $p-1$. Quare cum series geometrica $1; a; a^2; a^3; a^4; a^5; \text{etc.}$ ex terminis numero infinitis constet, necesse est, vt plures termini eadem exhibeant residua.

Coroll. 3.

5. Sint a^m et a^n duo eiusmodi termini, qui idem praebeant residuum r ; ita vt sit $a^m = mp + r$ et $a^n = np + r$ erit $a^m - a^n = (m-n)p$, ideoque differentia horum terminorum $a^m - a^n$ per p erit diuisibilis. Innumeris ergo modis differentia inter binos terminos progressionis geometricae propositae per numerum p erit diuisibilis.

Coroll. 4.

6. Si potestas a^m det residuum r , potestas vero a^n residuum s , fueritque $r + s = p$, quo casu dicimus residuorum r et s alterum alterius esse complementum, hoc casu summa potestatum $a^m + a^n$ per numerum p erit diuisibilis. Cum enim sit $a^m = mp + r$ et $a^n = np + s$, erit $a^m + a^n = (m+n)p + r + s = (m+n+1)p$, ideoque factorem habet p .

Theorema 2.

7. Si potestas a^m per p diuisa praebeat residuum r , et potestas a^n residuum s , potestas a^{m+n} residuum praebebit rs .

G 2

Demon.

Demonstratio.

Sit enim $a^m = mp + r$ et $a^n = np + s$, erit $a^{m+n} = mnp + mps + npr + rs$; ideoque si a^{m+n} per p diuidatur, residuum erit rs ; quod si maius fuerit quam p , subtrahendo p , quoties fieri potest, id ad residuum ipso diuisore p reducetur. Q. E. D.

Coroll. 1.

8. Cum ipsius radice a per p diuisae residuum exponi queat per a ; (si enim sit $a < p$, erit a residuum proprie sic dictum, sin autem $a > p$, nihilominus residuum per a exprimere licet, quia simul $a - p$, vel $a - np$ subintelligitur), si potestatis a^m per p diuisae residuum sit r , potestatis a^{m+1} residuum erit ar , simili modo potestatis a^{m+2} residuum erit a^2r .

$$\begin{array}{ccccccc} - & - & - & - & a^{m+3} & - & - & - & a^{3r} \\ & & & & & & & & \text{etc.} \end{array}$$

Coroll. 2.

9. Hinc etiam sequitur, si potestatis a^m per p diuisae residuum sit $= r$, fore potestatis a^{2m} residuum $= rr$, potestatis a^{3m} residuum $= r^3$; etc. Ita si potestatis a^m residuum sit $= 1$, erit omnium harum potestatum a^{2m} ; a^{3m} ; a^{4m} ; a^{5m} ; etc. idem quoque residuum 1.

Coroll. 3.

10. Quod si potestatis a^m per p diuisae residuum sit $= p - 1$, quod, ut vidimus, per -1 exponi potest: tum potestatis a^{2m} residuum erit $= +1$, potestatis a^{3m} residuum

residuum $= -1$, at potestatis a^{m} iterum $= +1$.
 Atque in genere potestatis a^{m} residuum erit, vel $+1$,
 si n sit numerus par, vel -1 , si n sit numerus impar.

Scholion.

11. Hinc colligitur modus, satis expedite residua
 inueniendi, quae ex diuisione cuiuscunque potestatis per
 numerum quemcunque relinquuntur. Veluti si residuum
 inuestigare velimus, quod ex diuisione huius potestatis
 7^{160} per numerum 641 oritur

potest.	residua	nempe cum potestas prima 7 relinquat 7,
7^1	7	potestas vero $7^2, 7^3, 7^4$ relinquat 49, 343
7^2	49	et 478, seu -163 ; huius quadratum 7^8 re-
7^3	343	linquet 163^2 seu 288, et quadratum huius
7^4	478	7^{16} relinquet 288^2 seu 255. Simili modo
7^8	288	potestas 7^{32} relinquet 255^2 seu 284, et
7^{16}	255	potestatis 7^{64} residuum erit -110 , et ex 7^{128}
7^{32}	284	oritur 110^2 seu -79 , quod residuum per
7^{64}	-110	284 multiplicatum, dabit residuum po-
7^{128}	-79	testatis $7^{128+32} = 7^{160}$, quod erit 640
7^{160}	-1	seu -1 .

Notamus ergo, si potestas 7^{160} per 641 diuidatur, resi-
 duum fore 640 , seu -1 , vnde concludimus potestatis
 7^{320} residuum fore $+1$. Ergo in genere potestatis
 7^{160n} per 641 diuisae residuum erit, vel $+1$, si n sit
 numerus par, vel -1 , si n sit numerus impar.

Theorema 3.

12. Si numerus a sit primus ad p , formeturque
 haec progressio geometrica $1; a; a^2; a^3; a^4; a^5; a^6; a^7; etc.$

innumeri in ea occurrent termini, qui per p diuisi relinquunt pro residuo 1 , et exponentes horum terminorum progressionem arithmeticam constituent.

Demonstratio.

Quia numerus terminorum est infinitus, plura autem diuersa residua oriri nequeunt, quam $p-1$, necesse est vt plures, immo infiniti, termini idem producant residuum r . Sint a^μ et a^ν duo huiusmodi termini, idem residuum r relinquentes, eritque $a^\mu - a^\nu$ per p diuisibile. At $a^\mu - a^\nu = a^\nu(a^{\mu-\nu} - 1)$, et cum hoc productum sit diuisibile per p , alter autem factor a^ν ad p sit primus, necesse est, alter factor $a^{\mu-\nu} - 1$ per p sit diuisibilis; vnde potestas $a^{\mu-\nu}$ per p diuisa residuum habebit $= 1$. Sit $\mu - \nu = \lambda$, vt potestatis a^λ residuum sit $= 1$, eritque omnium quoque harum potestatum $a^{2\lambda}$, $a^{3\lambda}$, $a^{4\lambda}$, $a^{5\lambda}$ etc. idem residuum $= 1$. Itaque vnitas erit residuum omnium harum potestatum:

1 ; a^λ , $a^{2\lambda}$; $a^{3\lambda}$; $a^{4\lambda}$; $a^{5\lambda}$; $a^{6\lambda}$; etc.

quarum exponentes in progressionem arithmeticam progrediuntur.

Coroll. 1.

13 . Inuenta ergo vnica potestate a^λ , quae per p diuisa residuum praebet $= 1$, infinitae inde aliae potestates exhiberi possunt, quae per p diuisae quoque vnitatem relinquant. Ac infima quidem huius generis potestas est $a^0 = 1$.

Coroll.

Coroll. 2.

14. Etiam si autem praeter unitatem nulla constet potestas ipsius a , quae per p diuisa unitatem pro residuo relinquat, tamen nouimus infinitas huiusmodi reuera dari potestates.

Coroll. 3.

15. Ex demonstratione porro patet, dari adeo potestatem a^λ residuum $=r$ praebentem, cuius exponents λ sit minor quam p . Si enim progressio geometrica tantum usque ad terminum a^{p-1} continuetur, quia terminorum numerus est $=p$, necesse est, ut saltem duo termini, qui sint a^μ et a^ν idem habeant residuum; unde cum potestas $a^{\mu-\nu}$ habitura sit residuum $=r$, ob $\mu < p$ et $\nu < p$, certe erit $\mu - \nu < p$.

Theorema 4.

16. Si potestas a^m per p diuisa, residuum relinquat $=r$, et potestatis altioris a^{m+n} residuum sit $=rs$, erit potestatis a^n , quae haec illam superat, residuum $=s$.

Demonstratio.

Praebet enim potestas a^n aliud residuum, puta $=t$, et cum potestatis a^m residuum sit $=r$, erit potestatis a^{m+n} residuum $=rt$, quod ipsi rs aequivalere deberet. Foret ergo $rt = rs + np$, siquidem ponamus residua r, t , esse ipso diuisore p minora. Effet ergo $t = s + \frac{np}{r}$: at cum a et p sint numeri inter se primi, omnia residua, quae ex potestatibus ipsius a
per

per p diuisis oriuntur, pariter erunt ad p prima, nisi forte sint $\equiv 1$, ideoque vt $\frac{n \cdot p}{r}$ fiat numerus integer, necesse est, vt $\frac{n}{r}$ sit numerus integer, puta $\equiv m$, foretque $t \equiv s + mp$, ideoque $t \equiv s$. Quare si potestatis a^h residuum sit $\equiv r$, et potestatis a^{h+v} residuum $\equiv rs$, hinc sequitur potestatis a^v residuum fore $\equiv s$.

Coroll. 1.

17. Si ergo $s \equiv 1$, seu si duae potestates a^h et a^{h+v} idem habeant residuum r , sequitur, si maior per minorem diuidatur, quoto a^v respondere residuum $\equiv 1$, quo ipso demonstratio praecedentis theorematis innitur.

Coroll. 2.

18. Si $r \equiv 1$ et $s \equiv 1$, seu si duae potestates a^h et a^{h+v} idem habeant residuum $\equiv 1$, tum etiam potestas a^v , cuius exponens est differentia illorum exponentum, pariter residuum $\equiv 1$ habebit.

Scholion.

19. Demonstratio huius theorematis etiam hoc modo confici potest. Cum a^h per p diuisum relinquat r , erit $a^h \equiv mp + r$, similique modo $a^{h+v} \equiv np + rs$; hinc erit $a^{h+v} - a^h s \equiv np - mps \equiv (n - ms)p$; ideoque numerus $a^{h+v} - a^h s \equiv a^h(a^v - s)$ erit per p diuisibilis: at alter factor a^h per p non est diuisibilis. Ergo alter $a^v - s$ erit per p diuisibilis, consequenter potestas a^v per p diuisa residuum dabit $\equiv s$.

Theo-

Theorema 5.

20. Si post unitatem a^λ fit minima potestas, quae per p diuisa unitatem relinquit, tum nullae aliae potestates idem residuum $= 1$ relinquent, nisi quae in hac progressionem geometricam occurrunt.

$1; a^\lambda, a^{2\lambda}; a^{3\lambda}; a^{4\lambda}, a^{5\lambda};$ etc.

Demonstratio.

Ponamus enim, aliam quampiam potestatem a^μ , si per p diuidatur, residuum quoque dare $= 1$, et cum fit $\mu > \lambda$, neque tamen multiplo cuiuspiam ipsius λ aequetur, hic exponentis μ ita exhiberi potest, ut fit $\mu = n\lambda + \delta$, vti fit $\delta < \lambda$: neque erit $\delta = 0$. Cum igitur tam potestas $a^{n\lambda}$, quam $a^\mu = a^{n\lambda + \delta}$, per p diuisa unitatem relinquat, per §. 18, haec quoque potestas a^δ unitatem pro residuo habebit, foretque ergo a^λ non minima potestas huius indolis contra hypothesin. Quare si a^λ fit minima potestas residuum $= 1$ praebens, nullae aliae potestates eadem proprietate erunt praeditae, nisi quarum exponentes sunt multipla ipsius λ .

Coroll. 1.

21. Si ergo progressionis geometricae $1, a, a^2, a^3, a^4,$ etc. iam secundus terminus a per p diuisus relinquat 1 , quod fit, si $a = np + 1$, tum omnes termini idem praebebunt residuum $= 1$: neque ergo in residuis vlli alii numeri praeter 1 occurrent.

Coroll. 2.

22. Si residuum tertii termini a^2 fit $= 1$, quod fit, si $a^2 = np + 1$, tum alterni termini $1, a^2, a^4, a^6,$ etc.

Tom. VII. Nou. Com. H quorum

quorum exponentes sunt pares, omnes residuum habebunt idem $\equiv 1$, reliqui vero termini, nisi a^r quoque residuum habeat $\equiv 1$, omnes alia praebebunt residua.

Coroll. 3.

23. Fieri ergo potest, ut in residuis multo pauciores numeri occurrant, quam numerus $p-1$ continet unitates: plures autem, quam $p-1$ diversi numeri occurrere non possunt.

Theorema 6.

24. Si potestas a^{2^n} , cuius exponens est numerus par, per numerum primum p diuisa, residuum $\equiv 1$ relinquit, tum potestas a^n per eundem numerum p diuisa, dabit residuum $\equiv +1$, vel $\equiv -1$.

Demonstratio.

Ponamus enim r esse residuum, quod in diuisione potestatis a^{2^n} per numerum primum p relinquitur, eritque potestatis a^{2^n} residuum $\equiv rr$, quod per hypothesein $\equiv 1$. Quare erit $rr \equiv 1 + mp$, et $rr - 1 \equiv mp$; unde cum $rr - 1 = (r + 1)(r - 1)$ sit diuisibile per p , alterutrum factorem $r + 1$ vel $r - 1$ per p diuisibilem esse oportet. Priori casu erit $r + 1 \equiv \alpha p$, et $r \equiv \alpha p - 1$, hincque $r \equiv -1$. Posteriori casu erit $r - 1 \equiv \alpha p$ et $r \equiv \alpha p + 1$, hincque $r \equiv +1$. Ergo si potestas a^{2^n} residuum praebeat $\equiv +1$, potestas a^n habebit vel residuum $\equiv +1$, vel $\equiv -1$, siquidem p sit numerus primus.

Coroll. 1.

25. Si igitur a^{2^n} fuerit minima potestas, quae per numerum primum p diuisa residuum relinquit $\equiv +1$,

$= +1$, tum potestas a^n residuum dabit $= -1$. Ergo si minimae potestatis a^λ residuum $= 1$ praebentis exponens λ sit numerus par, tum inter residua terminorum progressionis geometricae $1, a, a^2, a^3, a^4$, etc. etiam occurret numerus -1 .

Coroll. 2.

26. Sin autem minimae potestatis a^λ residuum $\neq 1$ praebentis exponens λ sit numerus impar, tum nulla omnino potestas residuum relinquet $= -1$. Si enim quaequam potestas, uti a^μ , daret residuum $= -1$, tum potestas $a^{2\mu}$ daret residuum $= +1$, foretque idcirco $2\mu = n\lambda$, et quia λ est numerus impar, foret $2\mu = 2m\lambda$, ideoque $\mu = m\lambda$. At potestas $a^{m\lambda}$ relinquit residuum $= +1$, neque ergo residuum -1 usquam occurrere potest.

Theorema 7.

27. Si a^λ fuerit minima potestas ipsius a , quae per numerum p diuisa, residuum praebet $= 1$, tum omnia residua, quae ex terminis progressionis geometricae $1, a, a^2, a^3, \dots, a^{\lambda-1}$, usque ad illam potestatem a^λ continuatae, resultant, erunt inter se inaequalia.

Demonstratio.

Si enim duae potestates, veluti a^μ et a^ν , quarum exponentes μ et ν sint minores, quam λ , idem darent residuum, tum earum differentia $a^\mu - a^\nu$ foret per p diuisibilis, ideoque potestas $a^{\mu-\nu}$ per p diuisa residuum relinqueret $= +1$, essetque idcirco $\mu - \nu < \lambda$, contra

H 2 hypo.

hypothefin; unde patet, omnes potestates, quarum exponentes sint minores, quam λ , diuersa praeberere residua.

Theorema. 8.

28. Si a^λ fuerit quaedam potestas ipsius a , quae per numerum p diuisa residuum producat $\equiv 1$, atque progressio geometrica in membra discerpatur, secundum potestates $a^\lambda, a^{2\lambda}, a^{3\lambda}, a^{4\lambda}$ etc. hoc modo:

$1, a, a^2 \dots a^{\lambda-1} \mid a^\lambda \dots a^{2\lambda-1} \mid a^{2\lambda} \dots a^{3\lambda-1} \mid a^{3\lambda} \dots a^{4\lambda-1} \mid$ etc.
ita ut quoduis membrum λ terminos contineat, tum in quolibet membro residua prodibunt eadem, atque eodem ordine recurrent.

Demonstratio.

Omnium enim membrorum termini primi $1, a^\lambda, a^{2\lambda}, a^{3\lambda}$ etc. idem praebent residuum $\equiv 1$. Termini deinde secundi omnium membrorum $a, a^{\lambda+1}, a^{2\lambda+1}, a^{3\lambda+1}$; etc. idem pariter dabunt residuum; sit enim r residuum ex termino a^r ortum, quia $a^{\lambda+r} = a^\lambda \cdot a^r$ erit residuum ex hoc termino ortum $\equiv 1 \cdot r = r$; similique modo patet, terminorum $a^{2\lambda+1}, a^{3\lambda+1}$ etc. residua fore $\equiv r$. Ac si in genere sit a^μ terminus quocumque primi membri, atque residuum ex eo ortum $\equiv r$, erit quoque termini $a^{n\lambda+\mu}$ residuum $\equiv r$, quia termini $a^{n\lambda}$ residuum est $\equiv 1$: hincque omnium membrorum termini analogi $a^{\lambda+\mu}, a^{2\lambda+\mu}, a^{3\lambda+\mu}$ etc. idem habebunt residuum.

Coroll.

Coroll. 1.

29. Quodsi ergo tantum terminorum in primo membro contentorum residua fuerint cognita, tum omnium quoque terminorum, qui reliqua membra constituunt, residua erunt cognita.

Coroll. 2.

30. Si enim proponatur terminus a^x , cuius exponens x sit numerus quantumvis magnus, eius residuum facile reperietur. Iste enim exponens x ad hanc formam $n\lambda + \mu$ reduci potest, ut sit $\mu < \lambda$, atque residuum termini a^x idem erit, quod termini a^μ .

Coroll. 3.

31. Hic autem numerus μ minor quam λ invenitur, si numerus x per λ diuidatur, tum enim residuum, quod in hac diuisione remanet, erit hic ipse numerus μ , qui quaeritur.

Coroll. 4.

32. Semper autem datur potestas a^λ , quae per p diuisa vnitatem relinquit, cuius exponens λ minor sit quam numerus propositus p , sicque ad residua omnium terminorum progressionis geometricae inuenienda, non opus est operationem ultra terminum a^p continuare.

Coroll. 5.

32. Si autem potestas a^λ sit minima earum, quae per numerum p diuisae vnitatem relinquunt; tunc

H 3

quia

quia singuli termini minores quam a^λ diuersa praebent residua, in residuis omnibus, neque plures, neque pauciores diuersi numeri occurrent quam λ . Igitur si λ fit minus quam $p-1$, non omnes numeri in residuis occurrent: sed quidam numeri plane nunquam in diuisione terminorum progressionis geometricae $1, a, a^2, a^3$ etc. remanere poterunt.

Coroll. 6.

34. Si igitur diuersitas residuorum spectetur, fieri potest, ut ex omnibus potestatibus ipsius a unicum tantum residuum, vel duo tantum residua diuersa, vel tria etc. prodeant, plura tamen nunquam quam $p-1$ locum habere possunt. Quotquot autem prodierint residua, inter ea semper unitas reperitur.

Theorema 9.

35. Si p fit numerus primus, et a primus ad p , atque omnes numeri ipso p minores reperiantur inter residua, quae ex diuisione omnium potestatum ipsius a per numerum primum p oriuntur, tum a^{p-1} erit minima potestas, quae per p diuisa unitatem relinquit.

Demonstratio.

Sit a^λ minima potestas, quae per p diuisa relinquat unitatem, atque ex praecedentibus patet, esse $\lambda < p(15)$. Iam cum numerus omnium residuorum diuersorum sit $= \lambda$, et omnium numerorum ipso p minorum $= p-1$, patet, si esset $\lambda < p-1$, non omnes nume-

numeros minores quam p in residuis occurrere; non igitur erit $\lambda < p-1$, neque vero est $\lambda > p-1$, quia alioquin non foret $\lambda < p$. Vnde relinquitur esse $\lambda = p-1$. Quocirca si omnes numeri ipso p minores in residuis occurrant, potestas a^{p-1} erit minima, quae per p diuisa unitatem relinquit.

Scholion.

36. Natura huius theorematis postulat, ut p sit numerus primus; nisi enim esset talis, fieri non posset, ut omnes numeri ipso p minores in residuis occurrerent. Quod quo clarius perspiciatur, perpendendum est, si p est numerus compositus, ad quem tamen a sit primus, nullam partem aliquotam ipsius p in residuis locum habere: nam si potestas quaequam a^m daret residuum r , quod esset pars aliquota ipsius p , ob $a^m = mp + r$, etiam ipsa potestas a^m diuisorem haberet r , ideoque nec ea, neque radix a esset numerus ad p primus, quod hypothese aduersatur.

Theorema 10.

37. Si numerus diuersorum residuorum, quae ex diuisione potestatum $1, a, a^2, a^3, a^4, a^5$, etc. per numerum primum p nascuntur, minor sit quam $p-1$, tum ad minimum totidem erunt numeri, qui non sunt residua, quot sunt residua.

Demonstratio.

Sit a^λ potestas minima, quae per p diuisa unitatem relinquat, ac sit $\lambda < p-1$, erit numerus omnium
resi-

residuorum diuerforum $\equiv \lambda$, ideoque minor quam $p-1$. Cum ergo numerus omnium numerorum ipso p minorum, sit $\equiv p-1$, patet dari numeros in casu proposito, qui in residuis non locum obtineant. Dico autem huiusmodi numerorum numerum ad minimum esse $\equiv \lambda$. Quod ut ostendatur, exponamus residua per ipsos terminos, ex quibus oriuntur, eruntque

haec residua $1, a, a^2, a^3, a^4 \dots a^{\lambda-1}$

quorum numerus $\equiv \lambda$, atque haec residua, si ad formam consuetam reducantur, omnia erunt minora quam p et inter se diuersa. Cum igitur sit $\lambda < p-1$ per hypothesin, dabitur certe numerus, qui in his residuis non reperitur. Sit talis numerus k ; iam dico si k non sit residuum, neque ak , neque a^2k , neque a^3k , etc. neque $a^{\lambda-1}k$ in residuis occurrere. Fac enim $a^\mu k$ esse residuum ex potestate a^α oriundum, foret $a^\alpha \equiv np + a^\mu k$, seu $a^\alpha - a^\mu k \equiv np$, ideoque $a^\alpha - a^\mu k \equiv a^\mu (a^{\alpha-\mu} - k)$ per p diuisibile. At a^μ per p non est diuisibile, esset ergo $a^{\alpha-\mu} - k$ per p diuisibile, seu potestas $a^{\alpha-\mu}$ per p diuisa, residuum relinqueret k , quod hypothesi repugnat. Ex quo patet, omnes hos numeros: $k, ak, a^2k, a^3k, \text{etc.}$
 $\dots a^{\lambda-1}k$, seu numeros inde deriuatos, non esse residua. At hi numeri, quorum multitudo $\equiv \lambda$, omnes sunt diuersi inter se; si enim duo, veluti $a^\mu k$ et $a^\nu k$, convenirent, ad idemque residuum r reducerentur, foret $a^\mu k \equiv mp + r$ et $a^\nu k \equiv np + r$, ideoque $a^\mu k - a^\nu k \equiv (m-n)p$, seu $(a^\mu - a^\nu)k \equiv (m-n)p$ esset per p diuisibile. Neque vero k per p est diuisibile, siquidem ponimus p numerum primum et $k < p$; esset $a^\mu - a^\nu$ per p diuisibilis, seu $a^{\mu-\nu}$ per p diuisum, unitatem relinqueret, cum tamen
 ob

ob $\mu < \lambda - 1$ et $\nu < \lambda - 1$, effct $\mu - \nu < \lambda$, quod effct absurdum. Ergo omnes illi numeri $k, ak, a^2k, a^3k, \dots, a^{\lambda-1}k$, si reducantur, erunt inter se diuersi, eorumque multitudo est $= \lambda$. Ad minimum ergo dantur λ numeri, qui in residuis locum non inueniunt, siquidem sit $\lambda < p - 1$.

Coroll. 1.

38. Cum igitur habeantur λ diuersi numeri, qui sunt residua, totidemque diuersi numeri, qui non sunt residua, omnesque sint minores quam p , illorum iunctim sumtorum numerus 2λ maior esse nequit, quam $p - 1$: quia non plures dantur numeri ipso p minores, quam $p - 1$.

Coroll. 2.

39. Si ergo a^λ sit minima potestas, quae per numerum primum p diuisa relinquit unitatem, fueritque $\lambda < p - 1$, tum certum est, non esse $\lambda > \frac{p-1}{2}$: erit ergo vel $\lambda = \frac{p-1}{2}$, vel $\lambda < \frac{p-1}{2}$.

Coroll. 3.

40. Ante vidimus exponentem istius potestatis minimae λ esse necessario minorem quam p ; Erit ergo vel $\lambda = p - 1$, vel $\lambda < p - 1$; hocque casu si $\lambda < p - 1$, simul nouimus, iam esse vel $\lambda = \frac{p-1}{2}$, vel $\lambda < \frac{p-1}{2}$. Atque adeo intra limites $p - 1$ et $\frac{p-1}{2}$ nullus continetur numerus, qui vnquam esse possit valor ipsius λ .

Theorema 2.

41 Si p fit numerus primus, atque a^λ minima potestas ipsius a , quae per p diuisa vnitatem relinquit, fueritque $\lambda < \frac{p-1}{2}$; tum fieri nequit, vt iste exponent λ fit maior quam $\frac{p-1}{2}$; eritque ergo vel $\lambda = \frac{p-1}{2}$, vel $\lambda < \frac{p-1}{2}$.

Demonstratio.

Cum a^λ fit minima potestas, quae per numerum primum p diuisa, vnitatem relinquit, plures in residuis non occurrunt numeri diuersi, quam λ , qui relinquuntur ex his terminis

$$1; a; a^2; a^3; a^4; \dots a^{\lambda-1}$$

si singuli per p diuidantur; quare cum fit $\lambda < p-1$ habebuntur $p-1-\lambda$ numeri, qui non sunt residua, quorum si vnus aliquis fit $=r$, vidimus hos omnes numeros

$$r; ar; a^2r; a^3r; a^4r \dots a^{\lambda-1}r$$

siquidem diuidendo per p ad numeros ipso p minores reducuntur, in residuis non contineri. Hinc autem tantum λ numeri ex residuis excluduntur; quare cum fit $\lambda < \frac{p-1}{2}$, erit $\lambda < p-1-\lambda$, ideoque praeter hos numeros alii insuper dantur, qui in residuis non continentur. Sit s huiusmodi numerus, qui neque fit residuum, neque in praecedente serie non-residuorum continetur; atque etiam hi omnes numeri

$$s; as; a^2s; a^3s; a^4s; \dots a^{\lambda-1}s$$

non erunt residua: hique numeri, vti in praecedente demonstratione ostendimus, omnes inter se erunt diuersi.

verfi. Neque vero vllus etiam horum numerorum, veluti $a^{\mu}s$, iam in praecedente ferie non-residuorum continetur, seu non est $a^{\mu}s = a^{\nu}s$. Nam si effet $a^{\nu}r = a^{\mu}s$, foret $s = a^{\nu-\mu}r$, vel $s = a^{\lambda+\nu-\mu}r$, siquidem effet $\mu > \nu$, vnde s iam in priori ferie contineretur contra hypothesin. Quocirca si $\lambda < \frac{p-1}{2}$, dantur ad minimum adhuc λ numeri, qui non sunt residua, sique cum λ habeamus residua, et 2λ non-residua, hique numeri omnes sint ipso p minores, fieri nequit, vt sit eorum summa 3λ maior quam $p-1$, seu non erit $\lambda > \frac{p-1}{3}$. Erit ergo vel $\lambda = \frac{p-1}{3}$, vel $\lambda < \frac{p-1}{3}$; siquidem fit $\lambda < \frac{p-1}{2}$: et p numerus primus.

Coroll. 1.

42. Si ergo non fit $\lambda < \frac{p-1}{3}$, tum certe erit $\lambda = \frac{p-1}{3}$, siquidem fit $\lambda < \frac{p-1}{2}$. At remota hac conditione, si nouerimus, non esse $\lambda < \frac{p-1}{3}$, tum necessario sequitur, esse vel $\lambda = \frac{p-1}{3}$, vel $\lambda = \frac{p-1}{2}$, vel $\lambda = p-1$.

Coroll. 2.

43. Siue autem fit $\lambda = \frac{p-1}{3}$, siue $\lambda = \frac{p-1}{2}$, potestas a^{p-1} per p diuisa, relinquit vnitatem. Si enim a^{λ} vnitatem relinquat, etiam $a^{2\lambda}$ et $a^{3\lambda}$ vnitatem pro residuo dabunt.

Theorema 12.

44. Si a^{λ} fit minima potestas ipsius a , quae per numerum primum p diuisa vnitatem relinquit, fueritque

I 2

$$\lambda > \frac{p-1}{3},$$

$\lambda < \frac{p-1}{4}$, tum certe non erit $a > \frac{p-1}{4}$, eritque ergo vel $\lambda = \frac{p-1}{4}$, vel $\lambda < \frac{p-1}{4}$.

Demonstratio.

Quia numerus omnium residuorum diuersorum, quae ex diuisione omnium potestatum ipsius a per numerum primum p proueniunt, est $=\lambda$, atque ex his terminis nascuntur: $1; a; a^2; a^3; a^4 \dots a^{\lambda-1}$; ob $\lambda < \frac{p-1}{4}$ habebuntur statim bis tot numeri, qui non sunt residua, qui ex his duabus progressionibus oriuntur

$$r; ar; a^2r; a^3r; a^4r \dots a^{\lambda-1}r$$

$$\text{et } s; as; a^2s; a^3s; a^4s \dots a^{\lambda-1}s$$

horum numerorum, tam residuorum, quam non-residuorum numerus, est $=3\lambda$, ideoque minor quam $p-1$, supererunt ergo adhuc numeri, qui non erunt residua. Sit t talis numerus, atque ut ante ostendimus, etiam hi omnes numeri

$$t; at; a^2t; a^3t; a^4t \dots a^{\lambda-1}t$$

non erunt residua, quorum numerus est $=\lambda$. At hi numeri non solum inter se erunt diuersi, cum p sit numerus primus, sed etiam a praecedentibus discrepant, sicque omnium horum numerorum, siue residuorum, siue non-residuorum multitudo est $=4\lambda$, et cum singuli hi numeri sint minores quam p ; impossibile est, ut sit $4\lambda > p-1$; eritque ergo vel $\lambda = \frac{p-1}{4}$, vel $\lambda < \frac{p-1}{4}$: siquidem sit, ut assumimus, $\lambda < \frac{p-1}{4}$ et p numerus primus.

Coroll.

Coroll. 1.

45. Simili modo demonstrabitur, si sit $\lambda < \frac{p-1}{4}$, tum impossibile esse, ut sit $\lambda > \frac{p-1}{5}$, foreque idcirco vel $\lambda = \frac{p-1}{5}$, vel $\lambda < \frac{p-1}{5}$.

Coroll. 2.

46. In genere etiam si constet esse $\lambda < \frac{p-1}{n}$, eodem modo demonstrabitur, fieri non posse, ut esset $\lambda > \frac{p-1}{n+1}$, eritque propterea vel $\lambda = \frac{p-1}{n+1}$, vel $\lambda < \frac{p-1}{n+1}$.

Coroll. 3.

47. Hinc patet omnium numerorum, qui residua esse nequeant, numerum esse vel $= 0$, vel $= \lambda$, vel $= 2\lambda$, vel alii cuiusque multiplo ipsius λ : si enim plures fuerint istiusmodi numeri quam $n\lambda$, tum ob unicum statim λ noui insuper accedunt, ut eorum omnium numerus fiat $= (n+1)\lambda$; at si hic nondum omnes numeri non-residua contineantur, denuo subito λ noui accedent.

Theorema 13.

48. Si p sit numerus primus, et a^λ minima potestas ipsius a , quae per p diuisa unitatem relinquit, erit exponens λ diuisor numeri $p-1$.

Demonstratio.

Numerus ergo omnium residuorum diuersorum est $= \lambda$, vnde numerus reliquorum numerorum ipso p

minorum, qui residua esse nequeunt, erit $=p-1-\lambda$, at hic numerus (47) est multipulum ipsius λ , puta $n\lambda$, ita ut sit $p-1-\lambda=n\lambda$, unde fit $\lambda=\frac{p-1}{n+1}$. Perspicuum ergo est, exponentem λ esse diuisorem numeri $p-1$, unde si non sit $\lambda=p-1$, certe parti cuidam aliquotae numeri $p-1$ exponens λ aequalis erit.

Theorema 14.

49. Si p sit numerus primus, et a primus ad p , tum potestas a^{p-1} per p diuisa unitatem relinquet.

Demonstratio.

Sit a^λ minima potestas ipsius a , quae per p diuisa unitatem relinquit, erit, ut vidimus, $\lambda < p$, atque insuper demonstrauius, esse vel $\lambda=p-1$, vel λ esse partem aliquotam numeri $p-1$. Priori casu constat propositum, atque potestas a^{p-1} per p diuisa unitatem relinquet. Posteriori casu, quo λ est pars aliquota numeri $p-1$, erit $p-1=n\lambda$, at cum potestas a^λ per p diuisa unitatem relinquat, etiam omnes hae potestates $a^{2\lambda}$, $a^{3\lambda}$, $a^{4\lambda}$ etc. ideoque et $a^{n\lambda}$, seu a^{p-1} , per p diuisae unitatem relinquent. Semper ergo potestas a^{p-1} per p diuisa unitatem relinquit.

Coroll. 1.

50. Quia potestas a^{p-1} per numerum primum p diuisa unitatem relinquit, formula $a^{p-1}-1$ per numerum primum p erit diuisibilis, siquidem a sit numerus ad p primus, seu si a non sit diuisibilis per p .

Coroll.

Coroll. 2.

51. Si ergo p fit numerus primus, omnes potestates exponentis $p-1$, veluti n^{p-1} per p diuisae, vel unitatem relinquent, vel nihil. LIQUA RARIET EUENIET.
 si n fit numerus ad p primus, hoc vero si ipse numerus n per p fuerit diuisibilis.

Coroll. 3.

52. Si p fit numerus primus, atque numeri a et b primi ad p , erit differentia potestatum $a^{p-1}-b^{p-1}$ per numerum p diuisibilis. Cum enim tam $a^{p-1}-1$, quam $b^{p-1}-1$, per p fit diuisibilis, etiam differentia harum formularum, id est $a^{p-1}-b^{p-1}$, per p erit diuisibilis.

Scholion.

53. En ergo nouam demonstrationem theorematis eximii, a Fermatio quondam prolata, quae maxime discrepat ab ea, quam in Comment. Acad. Petropol. Tomo VIII. dedi. Ibi enim euolutionem binomii $(a+b)^n$ in seriem modo *Newtoniano* in subsidium vocaui, quae consideratio a proposito non mediocriter abhorre videtur; hic vero idem theoremata ex solis potestatum proprietatibus demonstraui, vnde haec demonstratio magis naturalis videtur, cum praeterea nobis alias insignes proprietates circa residua potestatum, quando per numeros primos diuiduntur, manifestet. Patet etiam, si p fit numerus primus, non solum formulam $a^{p-1}-1$ per p esse diuisibilem, sed etiam interdum fieri posse, vt etiam forma simplicior $a^\lambda-1$
 per

per p sit diuisibilis, tumque exponentem λ esse partem aliquotam exponentis $p-1$.

Theorema 15.

54. Si q sit numerus primus, atque potestas a^q per numerum primum p diuisa unitatem relinquat, tum a^q erit minima potestas ipsius a , quae per p diuisa unitatem relinquit, nisi forte ipse numerus a per p diuisus unitatem relinquat.

Demonstratio.

Sit enim a^λ minima potestas ipsius a , quae per numerum primum p diuisa unitatem relinquat, atque nullae aliae potestates hac proprietate erunt praeditae, nisi $a^{2\lambda}$, $a^{3\lambda}$, $a^{4\lambda}$, etc. Verum nulli harum potestas a^q potest esse aequalis, nisi sit $\lambda=1$, cum q sit numerus primus, ideoque necesse est, ut sit $q=\lambda$, ideoque a^q minima potestas, quae per p diuisa unitatem relinquit. Excipitur autem casus, quo $\lambda=1$, seu quo ipse numerus a per p diuisus unitatem relinquit: hoc enim casu omnis potestas a^n , siue eius exponens n sit numerus primus, siue compositus, in diuisione per p facienda unitatem relinquet.

Coroll. 1.

55. Si ergo potestas a^q , cuius exponens est numerus primus, per numerum primum p diuisa unitatem relinquat, tum q erit pars aliquota numeri $p-1$, hocque casu formula a^q-1 per numerum primum p erit diuisibilis.

Coroll.

Coroll. 2.

56. Cum q fit pars aliquota numeri $p-1$, erit $p-1 = nq$, et $p = nq + 1$. Quodsi ergo formula $a^p - 1$, in qua q est numerus primus, diuisibilis fit per quempiam numerum primum p , habebit hic diuisor semper huiusmodi formam $p = nq + 1$, nisi sit $p = a - 1$: nam $a - 1$ semper est diuisor formulae $a^p - 1$.

Coroll. 3.

57. Formula ergo $a^q - 1$, existente q numero primo, praeter diuisorem $a - 1$ alios diuisores primos non admittit, nisi qui in hac forma $nq + 1$ contineantur; et cum q fit numerus primus, ideoque impar, nisi sit $q = 2$, pro n nonnisi numeri pares capi possunt, eruntque ergo omnes diuisores, si quos habet, in forma $2nq + 1$ contenti.

Coroll. 4.

58. Quia igitur formulae $a^q - 1$ diuisor est

$$a^{q-1} + a^{q-2} + a^{q-3} + a^{q-4} + \dots + a^2 + a + 1$$

haec forma in $2nq + 1$ continebitur, eritque ergo haec expressio: $a^{q-1} + a^{q-2} + a^{q-3} + \dots + a^2 + a$ per numerum primum q diuisibilis, quicumque numerus sit a , at si $a = q$, vel $a = mq$, hoc est manifestum per se.

Scholion I.

59. Hoc etiam manifestum est, si a non fit vel q vel mq ; tum enim formula inuenta abit in

$$a(a^{q-2} + a^{q-3} + a^{q-4} \dots + a + 1)$$

Tom. VII. Nou. Com.

K

cuius

cuius factor posterior, qui transit in $\frac{a^{q-1}-1}{a-1}$, per q est diuisibilis: quod quidem per se est euidentis; nam cum q sit numerus primus, per eum formula $a^{q-1}-1$ est diuisibilis; eademque etiam per $a-1$ diuisa, manebit per q diuisibilis, nisi $a-1$ diuisorem habeat q , qui casus iam ante est exceptus. Notandum enim est, formam $a^{q-1}+a^{q-2}+a^{q-3}\dots+a^2+a+1$ ea-tenus tantum in forma $2nq+1$ contineri, quatenus illa est vel numerus primus, vel ex numeris primis eiusdem formae $2nq+1$ compositus. At si illa formula ipsa iam habeat factorem $a-1$, per quem forma a^q-1 est diuisibilis, tum ea cum forma $2nq+1$ non conueniet. Sed si $a-1=mq$, vel $a=mq+1$, tum ipsa illa formula per q erit diuisibilis, quia terminorum numerus $=q$, neque ergo illa in forma $2nq+1$ continebitur.

Scholion 2.

60. Plurimum autem interest, nosse diuisores formulae a^q-1 , quando q est numerus primus, quoniam ii alias, excepto diuisore $a-1$, qui sponte se prodit, difficillime inuestigantur, fietique adeo potest, vt saepe huiusmodi formula, postquam est per $a-1$ diuisa, fiat numerus primus. At si q non est numerus primus, sed ipse diuisores habeat m, n , tum manifesto erunt hae formulae a^m-1 et a^n-1 diuisores formulae a^q-1 . His ergo casibus inuestigatio vltiorum diuisorum reducitur ad formulas a^m-1 et a^n-1 , in quibus exponentes m et n sunt numeri primi. Nouimus igitur, si quis ten-
tando

tando voluerit, diuifores formulæ $a^q - 1$ inueftigare, tentamen cum nullis aliis numeris primis, nifi qui in forma $2nq + 1$ contineantur, inftituendum eſſe, quo ipſo operatio alias difficillima, non mediocriter contrahitur.

Theorema 16.

61. Si poteſtas a^m , per numerum p diuiſa, reſiduum relinquat $= r$, tum etiam poteſtas $(a \pm \alpha p)^m$, per p diuiſa, idem relinquet reſiduum r .

Demonſtratio.

Si poteſtas $(a \pm \alpha p)^m$ euoluatur, prodibit
 $a^m \pm m\alpha a^{m-1}p + \frac{m(m-1)}{1 \cdot 2} \alpha^2 a^{m-2}p^2 \pm$ etc.
 cuius omnes termini, præter primum, per p ſunt diuiſi-
 biles: vnde hæc quantitas per p diuiſa idem relinquet
 reſiduum, ac ſi ſolus primus terminus a^m per p diui-
 deretur. Ergo cum poteſtas a^m reſiduum relinquat $= r$,
 etiam poteſtas $(a \pm \alpha p)^m$ reſiduum relinquet $= r$.

Coroll. 1.

62. Si m fit numerus par, demonſtratio etiam
 valet pro formula $(-a \pm \alpha p)^m$, hoc ergo caſu etiam
 formula $(\alpha p - a)^m$, per p diuiſa, idem relinquit reſiduum
 r , quod formula a^m relinquit.

Coroll. 2.

63. At ſi m fit numerus impar, quia formula
 $-a^m$ per p diuiſa reſiduum relinquit $= -r$, etiam for-
 mula $(\alpha p - a)^m$ reſiduum relinquet $= -r$.

Theorema 17.

64. Si fuerit $a = c^n + \alpha p$, tum formula $a^{\frac{p-1}{n}}$, per numerum primum p diuisa, unitatem relinquet, siquidem sit n diuisor numeri $p-1$.

Demonstratio.

Cum sit $a = c^n + \alpha p$, potestas $a^{\frac{p-1}{n}}$, seu $(c^n + \alpha p)^{\frac{p-1}{n}}$ per p diuisa, idem relinquit residuum, ac potestas $c^{n \cdot \frac{p-1}{n}}$ seu c^{p-1} , at ob p numerum primum, potestas c^{p-1} per p diuisa unitatem relinquit, ergo etiam potestas $a^{\frac{p-1}{n}}$ unitatem relinquet, siquidem sit $a = c^n + \alpha p$, neque tamen a vel c diuisibile fuerit per p .

Coroll. 1.

65. Ex hoc ergo theoremate cognoscuntur casus, quibus potestates numerorum, quarum exponentes sunt minores quam $p-1$, si per numerum primum p diuisantur, unitatem relinquant.

Coroll. 2.

66. Si ergo sit $a = cc + \alpha p$, existente p numero primo, tum potestas $a^{\frac{p-1}{2}}$ per p diuisa unitatem relinquet, seu formula $a^{\frac{p-1}{2}} - 1$ per p erit diuisibilis. Cum autem p sit numerus primus, nisi sit $= 2$, semper exponens $\frac{p-1}{2}$ erit numerus integer.

Coroll. 3.

67. Si sit $a = c^3 + \alpha p$, tum potestas $a^{\frac{p-1}{3}}$ per p diuisa unitatem relinquet, seu haec forma $a^{\frac{p-1}{3}} - 1$ per

per p erit diuisibilis. Hic casus locum habet, si numerus primus p ita sit comparatus, ut $p-1$ per 3 sit diuisibile.

Theorema 18.

68. Si sit $ab^n = c^n + ap$, et p numerus primus, tum potestas $a^{\frac{p-1}{n}}$ per p diuisa unitatem relinquet, siquidem $\frac{p-1}{n}$ fuerit numerus integer.

Demonstratio.

Potestas $(c^n + ap)^{\frac{p-1}{n}}$, seu $a^{\frac{p-1}{n}}b^{p-1}$, per p diuisa idem relinquit residuum, quod potestas $c^{n \cdot \frac{p-1}{n}} = c^{p-1}$, at haec potestas unitatem relinquit, ergo et potestas $a^{\frac{p-1}{n}}b^{p-1}$. Huius autem factor b^{p-1} pariter unitatem relinquit; ergo necesse est, alterum quoque factorem $a^{\frac{p-1}{n}}$, si per p diuidatur, unitatem relinque-
re, nisi sit b vel c diuisibile per p .

Coroll. 1.

69. Si ergo sit $ab^n = c^n + ap$, seu $ab^n - c^n$, siue $c^n - ab^n$, per numerum primum p diuisibile, tum haec quoque formula $a^{\frac{p-1}{n}} - 1$ per p erit diuisibilis.

Coroll. 2.

70. Cum p sit numerus primus, ponatur $p = mn + 1$, atque si fuerit haec formula $ab^n - c^n$, seu $c^n - ab^n$, per p diuisibilis, tum etiam haec formula $a^m - 1$ per numerum primum p erit diuisibilis.

Coroll. 3.

71. Dummodo ergo pro b et c eiusmodi numeri dentur, vt $ab^n - c^n$, seu $c^n - ab^n$ diuisionem per numerum primum $p = mn + 1$ admittat, tum certum est, hanc formulam $a^m - 1$ per eundem numerum primum $p = mn + 1$ esse diuisibilem.

Theorema 19.

72. Si formula $a^m - 1$ fuerit diuisibilis per numerum primum $p = mn + 1$, tum semper dantur numeri x et y eiusmodi, vt $ax^n - y^n$ sit per eundem numerum primum p diuisibilis.

Demonstratio.

Cum enim x^{mn} et y^{mn} per p diuisae unitatem relinquunt, formula $a^m x^{mn} - y^{mn}$ semper erit per p diuisibilis, dummodo neque x , neque y , per p sit diuisibile. Cum iam per factores sit $a^m x^{mn} - y^{mn} = (ax^n - y^n) (a^{m-1} x^{m(n-1)} + a^{m-2} x^{m(n-2)} y^n + a^{m-3} x^{m(n-3)} y^{2n} + \dots + y^{m(n-1)})$ si quis neget factorem primum $ax^n - y^n$ vnquam esse per p diuisibilem, is affirmare cogitur, alterum factorem semper esse per p diuisibilem, dummodo pro x et y non capiantur numeri per p diuisibiles. Retineat x valorem quemcunque, at pro y ponamus successiue numeros 1, 2, 3, 4, vsque ad $p - 1 = mn$, ne vnquam obtineat valorem per p diuisibilem, sitque breuitatis gratia

$A = a$

$$\begin{aligned}
 A &= a^{m-1} x^{mn-n} + a^{m-2} x^{mn-2n} + \dots + 1 \\
 B &= a^{m-1} x^{mn-n} + a^{m-2} x^{mn-2n} 2^n + \dots + 2^{mn-n} \\
 C &= a^{m-1} x^{mn-n} + a^{m-2} x^{mn-2n} 3^n + \dots + 3^{mn-n} \\
 &\vdots \\
 &\vdots \\
 &\vdots \\
 N &= a^{m-1} x^{mn-n} + a^{m-2} x^{mn-2n} (mn)^n + \dots + (mn)^{mn-n}
 \end{aligned}$$

ac forent omnes hae quantitates A, B, C, N, quae progressionem algebraicam ordinis $mn-n$ constituunt, per p diuisibiles, hincque etiam earum differentiae primae, secundae, tertiae et ordinis cuiusuis. At huius seriei differentia ordinis $mn-n$, quae tantum per terminos $mn-n-1$ seriei definitur, neque adeo terminum $(mn+1)^{mn-n}$, seu p^{mn-n} inuoluit, quia p non potest esse valor ipsius y , est uti constat:

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot \dots \cdot (mn-n)$$

quae aperte non est per numerum primum $p=mn+1$ diuisibilis, quia nullos alios habet diuisores primos, nisi qui sint minores quam $mn-n$. Cum igitur haec differentia ordinis $mn-n$ non sit diuisibilis per p , sequitur non omnes terminos seriei A, B, C, D, N esse per p diuisibiles. Illo igitur casu, vel illis casibus ipsius y , quibus termini huius seriei non sunt per p diuisibiles, necessario alter factor ax^n-y^n per p erit diuisibilis,

Corol-

Corollarium 1.

73. Quicumque ergo numerus pro x sumatur, modo per p non diuisibilis, pro y semper datur valor $< p$, qui reddit formulam $ax^n - y^n$ per p diuisibilem. Similique modo, si pro y numerus pro lubitu assumatur, demonstrari potest, semper pro x eiusmodi numerum $< p$ inueniri posse, quo eadem formula per p diuisibilis euadat.

Coroll. 2.

74. Si ergo $a^m - 1$ fuerit diuisibile per numerum primum $mn + 1 = p$, atque pro x capiatur numerus quicumque b per p non diuisibilis, semper inueniri potest numerus y , vt haec forma $ab^n - y^n$, seu $y^n - ab^n$, fiat per $p = mn + 1$ diuisibilis.

Coroll. 3.

75. Simili modo si forma $a^m - 1$ fuerit diuisibilis per numerum primum $p = mn + 1$, atque pro y capiatur numerus quicumque c per p non diuisibilis, semper inueniri poterit numerus x , vt haec forma $ax^n - c^n$, seu $c^n - ax^n$, fiat per $p = mn + 1$ diuisibilis.

Theorema 20.

76. Si haec forma $ab^n - c^n$, vel $c^n - ab^n$, fuerit diuisibilis per numerum primum $p = mn + 1$, tum sumto numero d pro lubitu, dummodo per p non fit diuisibilis

diuisibilis, semper inueniri potest numerus x , vt vel haec forma ax^n-d^n , vel haec ad^n-x^n , vel d^n-ax^n , vel x^n-ad^n fiat per eundem numerum primum $p=mn+1$ diuisibilis.

Demonstratio.

Cum haec forma ab^n-c^n , vel c^n-ab^n sit per numerum primum $p=mn+1$ diuisibilis, tum etiam hic numerus a^m-1 per eundem numerum primum $p=mn+1$ erit diuisibilis. (71) Verum si a^m-1 per p est diuisibilis, sumto numero quocunque d per p non diuisibili, dabitur numerus x , vt vel haec forma ax^n-d^n , vel etiam haec ad^n-x^n , vel d^n-ax^n , vel x^n-ad^n fiat quoque per numerum primum $p=mn+1$ diuisibilis.

Corollarium.

77. Posito ergo $d=1$, si formulae ab^n-c^n diuisor sit numerus primus $p=mn+1$, tum dabitur numerus x , vt vel haec forma ax^n-1 , vel $a-x^n$, vel x^n-a fiat per eundem numerum primum p diuisibilis.

Scholion.

78. Theorema vndeicesimum, quod inuersum est theorematis duodeicesimi, iam alibi proposueram, sed sine demonstratione, et tametsi tum eius demonstrationem multis modis tentavi, eam tamen inuenire non potui, donec in methodum hic vsitatam incidi:

82 DE RESIDUIS EX DIVISIONE POTEST. etc.

quae igitur eo magis notatu digna videtur, cum dubium fit nullum, quin eadem ad multa alia numerorum arcana viam sit patefactura. Haec quoque methodus, quae in consideratione differentiarum continetur, nuper mihi insigni viui fuit, dum eius beneficio tandem pulcherrimi theorematis Fermatiani, quo omnis numerus primus formae $4n + 1$ aggregatum duorum quadratorum esse affirmatur, demonstrationem sum consecutus; ad quam ante nullo alio modo peruenire potui.
