1761

Theoremata circa residua ex divisione potestatum relicta

Leonhard Euler

THEOREMATA
CIRCA RESIDVA EX DIVISIONE POTESTATVM RELICTA.

Auctore

L. EVLERO.

Theorema. I.

1.

Si p sit 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 sit 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. 1.

2. Si igitur singuli termini progressionis geometricae

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

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 $p+r$ aequiualet 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 $1; a; a^2; a^3; a^4; a^5;$ etc, ex terminis numero infinitis conſtet, neceſſe eſt, vt plures termini eadem exhibeant reſidua.

Coroll. 3.

5. Sint a^μ et a^ν duo eiusmodi termini, qui idem praebeant reſiduum r; ita vt ſit $a^\mu = mp+r$ et $a^\nu = np+r$ erit $a^\mu - a^\nu = (m-n)p$, ideoque differentia horum terminorum $a^\mu - a^\nu$ 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^μ det reſiduum r, poteſtas vero a^ν reſiduum s, ſueritque $r+s=p$, quo caſu dicimus reſiduorum r et s alterum alterius eſſe complementum, hoc caſu ſumma poteſtatum $a^\mu + a^\nu$ per numerum p erit diuiſibilis. Cum enim ſit $a^\mu = mp+r$ et $a^\nu = np+s$, erit $a^\mu + a^\nu = (m+n)p+r+s = (m+n+1)p$, ideoque factorem habet p.

Theorema 2.

7. Si poteſtas a^μ per p diuiſa praebeat reſiduum r, et poteſtas a^ν reſiduum s, poteſtas $a^{\mu+\nu}$ reſiduum praebebit rs.

Demonstratio.

Sit enim $a^{\mu} = mp + r$ et $a^{\nu} = np + s$, erit $a^{\mu+\nu} = mnpp + mps + npr + rs$; ideoque si $a^{\mu+\nu}$ 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 radicis 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^{μ} per p diuisae residuum sit r, potestatis $a^{\mu+1}$ residuum erit ar, simili modo potestatis $a^{\mu+2}$ residuum erit $a^2 r$

\- - - - $a^{\mu+3}$ - - - - $a^3 r$

etc.

Coroll. 2.

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

Coroll. 3.

10. Quodsi potestatis a^{μ} per p diuisae residuum sit $= p - 1$, quod, vt vidimus, per -1 exponi potest: tum potestatis $a^{2\mu}$ residuum erit $= +1$, potestatis $a^{3\mu}$ residuum

residuum $= -1$, at potestatis $a^{\frac{pp}{2}}$ iterum $= +1$. Atque in genere potestatis $a^{\frac{pp}{2}n}$ 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 $7^2, 7^3, 7^4$ relinquant 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.

Nouimus ergo, si potestas 7^{160} per 641 diuidatur, residuum 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:

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

quarum exponentes in progressione arithmetica 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. Etiamsi autem praeter vnitatem nulla constet potestas ipsius a, quae per p diuisa vnitatem pro residuo relinquat, tamen nouimus infinitas huiusmodi re vera dari potestates.

Coroll. 3.

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

Theorema 4.

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

Demonstratio.

Praebeat enim potestas a^{ν} aliud residuum, puta $= t$, et cum potestatis a^{μ} residuum sit $= r$, erit potestatis $a^{\mu+\nu}$ residuum $= rt$, quod ipsi rs aequiualere deberet. Foret ergo $rt = rs + np$, siquidem ponamus residua r, t, esse ipso diuisore p minora. Esset 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 $= 1$, ideoque vt $\frac{np}{r}$ fiat numerus integer, neceſſe eſt, vt $\frac{n}{r}$ ſit numerus integer, puta $= m$, foretque $t = s + mp$, ideoque $t = s$. Quare ſi poteſtatis a^μ reſiduum ſit $= r$, et poteſtatis $a^{\mu+\nu}$ reſiduum $= rs$, hinc ſequitur poteſtatis a^ν reſiduum fore $= s$.

Coroll. 1.

17. Si ergo $s = 1$, ſeu ſi duae poteſtates a^μ et $a^{\mu+\nu}$ idem habeant reſiduum r, ſequitur, ſi maior per minorem diuidatur, quoto a^ν reſpondere reſiduum $= 1$, quo ipſo demonſtratio praecedentis theorematis innititur.

Coroll. 2.

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

Scholion.

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

Theo-

Theorema 5.

20. Si post vnitatem a^λ sit minima potestas, quae per p diuisa vnitatem relinquit, tum nullae aliae potestates idem residuum $=1$ relinquent, nisi quae in hac progressione geometrica 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 sit $\mu > \lambda$, neque tamen multiplo cuipiam ipsius λ aequetur, hic exponens μ ita exhiberi potest, vt sit $\mu = n\lambda + \delta$, vti sit $\delta < \lambda$: neque erit $\delta = 0$. Cum igitur tam potestas $a^{n\lambda}$, quam $a^\mu = a^{n\lambda+\delta}$, per p diuisa vnitatem relinquat, per §. 18, haec quoque potestas a^δ vnitatem pro residuo habebit, foretque ergo a^λ non minima potestas huius indolis contra hypothesin. Quare si a^λ sit 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 sit $=1$, quod fit, si $a^2 = np + 1$, tum alterni termini $1, a^2, a^4, a^6$, etc.

quorum exponentes sunt pares, omnes residuum habebunt idem $= 1$, reliqui vero termini, nisi a^{ι} quoque residuum habeat $= 1$, omnes alia praebebunt residua.

Coroll. 3.

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

Theorema 6.

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

Demonstratio.

Ponamus enim r esse residuum, quod in diuisione potestatis a^{n} per numerum primum p relinquitur, eritque potestatis a^{2n} residuum $= rr$, quod per hypothesin $= 1$. Quare erit $rr = 1 + mp$, et $rr - 1 = mp$; vnde 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 $r+1 = \alpha p$, et $r = \alpha p - 1$, hincque $r = -1$. Posteriori casu erit $r-1 = \alpha p$ et $r = \alpha p + 1$, hincque $r = +1$. Ergo si potestas a^{2n} residuum praebeat $= +1$, potestas a^{n} habebit vel residuum $= +1$, vel $= -1$, siquidem p sit numerus primus.

Coroll. 1.

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

$\equiv +1$, tum potestas a^n residuum dabit $\equiv -1$. Ergo si minimae potestatis a^λ residuum $\equiv 1$ 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 1 praebentis exponens λ sit numerus impar, tum nulla omnino potestas residuum relinquet $\equiv -1$. Si enim quaepiam potestas, uti a^μ, daret residuum $\equiv -1$, tum potestas $a^{2\mu}$ daret residuum $\equiv +1$, 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 $\equiv +1$, neque ergo residuum -1 vsquam occurrere potest.

Theorema 7.

27. Si a^λ fuerit minima potestas ipsius a, quae per numerum p diuisa, residuum praebet $\equiv 1$, tum omnia residua, quae ex terminis progressionis geometricae $1, a, a^2, a^3 \ldots\ldots a^{\lambda-1}$, vsque 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 $\equiv +1$, essetque idcirco $\mu - \nu < \lambda$, contra

hypotheſin; vnde patet, omnes poteſtates, quarum exponentes ſint minores, quam λ, diuerſa praebere reſidua.

Theorema. 8.

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

$$1, a, a^2 \ldots a^{\lambda-1} \,|\, a^\lambda \ldots a^{2\lambda-1} \,|\, a^{2\lambda} \ldots a^{3\lambda-1} \,|\, a^{3\lambda} \ldots a^{4\lambda-1} \,|\, \text{etc.}$$

ita vt quoduis membrum λ terminos contineat, tum in quolibet membro reſidua prodibunt eadem, atque eodem ordine recurrent.

Demonſtratio.

Omnium enim membrorum termini primi 1, a^λ, $a^{2\lambda}$, $a^{3\lambda}$ etc. idem praebent reſiduum $= 1$. Termini deinde ſecundi omnium membrorum a, $a^{\lambda+r}$; $a^{2\lambda+1}$; $a^{3\lambda+1}$; etc. idem pariter dabunt reſiduum; ſit enim r reſiduum ex termino a^1 ortum, quia $a^{\lambda+1} = a^\lambda . a^1$ erit reſiduum ex hoc termino ortum $= 1 . r = r$; ſimilique modo patet, terminorum $a^{2\lambda+1}$, $a^{3\lambda+1}$ etc. reſidua fore $= r$. Ac ſi in genere ſit a^μ terminus quotuscunque primi membri, atque reſiduum ex eo ortum $= r$, erit quoque termini $a^{n\lambda+\mu}$ reſiduum $= r$, quia termini $a^{n\lambda}$ reſiduum eſt $= 1$: 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 quantumuis magnus, eius residuum facile reperietur. Iste enim exponens x ad hanc formam $n\lambda+\mu$ reduci potest, vt sit $\mu<\lambda$, atque residuum termini a^x idem erit, quod termini a^μ.

Coroll. 3.

31. Hic autem numerus μ minor quam λ inuenitur, 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 vltra terminum a^p continuare.

Coroll. 5.

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

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 sit minus quam $p-1$, non omnes numeri in residuis occurrent: sed quidam numeri plane nunquam in divisione terminorum progressionis geometricae $1, a, a^2, a^3$ etc. remanere poterunt.

Coroll. 6.

34. Si igitur diuersitas residuorum spectetur, fieri potest, vt ex omnibus potestatibus ipsius a vnicum 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 vnitas reperitur.

Theorema 9.

35. Si p sit 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 vnitatem relinquit.

Demonstratio.

Sit a^λ minima potestas, quae per p diuisa relinquat vnitatem, 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 diviſa vnitatem relinquit.

Scholion.

36. Natura huius theorematis poſtulat, vt p ſit numerus primus; niſi enim eſſet talis, fieri non poſſet, vt 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 quaepiam a^{μ} daret reſiduum r, quod eſſet pars aliquota ipſius p, ob $a^{\mu} = mp + r$, etiam ipſa poteſtas a^{μ} diuiſorem haberet r, ideoque nec ea, neque radix a eſſet numerus ad p primus, quod hypotheſi 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 vnitatem relinquat, ac ſit $\lambda < p-1$, erit numerus omnium reſi-

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

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

quorum numerus $= \lambda$, 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 $a^\alpha = np + a^\mu k$, ſeu $a^\alpha - a^\mu k = np$, ideoque $a^\alpha - a^\mu k = a^\mu(a^{\alpha-\mu} - k)$ 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, etc. $\ldots\ldots a^{\lambda-1}k$, ſeu numeros inde deriuatos, non eſſe reſidua. At hi numeri, quorum multitudo $= \lambda$, omnes ſunt diuerſi inter ſe; ſi enim duo, veluti $a^\mu k$ et $a^\nu k$, conuenirent, ad idemque reſiduum r reducerentur, foret $a^\mu k = mp + r$ et $a^\nu k = np + r$, ideoque $a^\mu k - a^\nu k = (m-n)p$, ſeu $(a^\mu - a^\nu)k = (m-n)p$ 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, vnitatem relinqueret, cum tamen

ob

ob $\mu < \lambda - 1$ et $\nu < \lambda - 1$, esset $\mu - \nu < \lambda$, quod esset absurdum. Ergo omnes illi numeri k, ak, a^2k, a^3k .... $a^{\lambda-1}k$, 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 vnitatem, 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 sit numerus primus, atque a^λ minima potestas ipsius a, quae per p diuisa vnitatem relinquit, fieritque $\lambda < \frac{p-1}{2}$; tum fieri nequit, vt iste exponens λ sit maior quam $\frac{p-1}{2}$; eritque ergo vel $\lambda = \frac{p-1}{2}$, vel $\lambda < \frac{p-1}{2}$.

Demonstratio.

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

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

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

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

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

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

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

verſi. Neque vero vllus etiam horum numerorum, veluti $a^{\mu}s$, iam in praecedente ſerie non-reſiduorum continetur, ſeu non eſt $a^{\mu}s = a^{\nu}s$. Nam ſi eſſet $a^{\nu}r = a^{\mu}s$, foret $s = a^{\nu-\mu}r$, vel $s = a^{\lambda+\nu-\mu}r$, ſiquidem eſſet $\mu > \nu$, vnde s iam in priori ſerie 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 ſit $\lambda < \frac{p-1}{2}$: et p numerus primus.

Coroll. 1.

42. Si ergo non ſit $\lambda < \frac{p-1}{3}$, tum certe erit $\lambda = \frac{p-1}{3}$, ſiquidem ſit $\lambda < \frac{p-1}{2}$. 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 ſit $\lambda = \frac{p-1}{3}$, 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} ſit minima poteſtas ipſius a, quae per numerum primum p diuiſa vnitatem relinquit, fueritque

$\lambda < \frac{p-2}{4}$, 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: $1; a; a^2; a^3; a^4 \ldots\ldots a^{\lambda-1}$: ob $\lambda < \frac{p-1}{3}$ habebuntur statim bis tot numeri, qui non sunt residua, qui ex his duabus progressionibus oriuntur

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

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 vt ante ostendimus, etiam hi omnes numeri

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

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, vt sit $4\lambda > p-1$; eritque ergo vel $\lambda = \frac{p-1}{4}$, vel $\lambda < \frac{p-1}{4}$: siquidem sit, vt assumsimus, $\lambda < \frac{p-1}{3}$ et p numerus primus.

Coroll.

Coroll. 1.

45. Simili modo demonstrabitur, si sit $\lambda < \frac{p-1}{4}$, tum impossibile esse, vt 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, vt 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 cuicunque multiplo ipsius λ: si enim plures fuerint istiusmodi numeri quam $n\lambda$, tum ob vnicum statim λ noui insuper accedunt, vt 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 vnitatem 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 multiplum ipſius λ, puta $n\lambda$, ita vt ſit $p-1-\lambda=n\lambda$, vnde fit $\lambda=\frac{p-1}{n+1}$. Perſpicuum ergo eſt, exponentem λ eſſe diuiſorem numeri $p-1$, vnde 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 vnitatem relinquet.

Demonſtratio.

Sit a^λ minima poteſtas ipſius a, quae per p diviſa vnitatem relinquit, erit, vt vidimus, $\lambda<p$, atque inſuper demonſtrauimus, 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 vnitatem relinquet. Poſteriori caſu, quo λ eſt pars aliquota numeri $p-1$, erit $p-1=n\lambda$, at cum poteſtas a^λ per p diuiſa vnitatem 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 vnitatem relinquent. Semper ergo poteſtas a^{p-1} per p diuiſa vnitatem relinquit.

Coroll. 1.

50. Quia poteſtas a^{p-1} per numerum primum p diuiſa vnitatem 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 sit numerus primus, omnes potestates exponentis $p-1$, veluti n^{p-1} per p diuisae, vel vnitatem relinquent, vel nihil. Illud scilicet euenit, si n sit numerus ad p primus, hoc vero si ipse numerus n per p fuerit diuisibilis.

Coroll. 3.

52. Si p sit 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 sit diuisibilis, etiam differentia harum formularum, id est $a^{p-1}-b^{p-1}$, per p erit divisibilis.

Scholion.

53. En ergo nouam demonstrationem theorematis eximii, a Fermatio quondam prolati, 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 abhorrere videtur; hic vero idem theorema 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 sit 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 vnitatem relinquat, tum a^q erit minima potestas ipsius a, quae per p diuisa vnitatem relinquit, nisi forte ipse numerus a per p diuisus vnitatem relinquat.

Demonstratio.

Sit enim a^λ minima potestas ipsius a, quae per numerum primum p diuisa vnitatem 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, vt sit $q = \lambda$, ideoque a^q minima potestas, quae per p diuisa vnitatem relinquit. Excipitur autem casus, quo $\lambda = 1$, seu quo ipse numerus a per p diuisus vnitatem relinquit: hoc enim casu omnis potestas a^n, siue eius exponens n sit numerus primus, siue compositus, in diuisione per p facienda vnitatem relinquet.

Coroll. 1.

55. Si ergo potestas a^q, cuius exponens est numerus primus, per numerum primum p diuisa vnitatem 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 sit pars aliquota numeri $p-1$, erit $p-1=nq$, et $p=nq+1$. Quodsi ergo formula a^q-1, in qua q est numerus primus, diuisibilis sit 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^q-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 sit 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

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

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

Scholion 1.

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

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

cuius factor posterior, qui transit in $\frac{a^{q-1}-1}{a-1}$, per q est diuisibilis: quod quidem per se est euidens; 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 $a^{q-1}+a^{q-2}+a^{q-3}\ldots\ldots+a^2+a+1$ eatenus 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, fierique 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 vlteriorum diuisorum reducitur ad formulas a^m-1 et a^n-1, in quibus exponentes m et n sunt numeri primi. Nouimus igitur, si quis tentando

tando voluerit, diuisores formulae $a^q - 1$ inuestigare, tentamen cum nullis aliis numeris primis, nisi qui in forma $2nq + 1$ contineantur, instituendum 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

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

cuius omnes termini, praeter primum, per p sunt diuisibiles: vnde haec quantitas per p diuisa idem relinquet residuum, ac si solus primus terminus a^m per p diuideretur. Ergo cum potestas a^m residuum relinquat $= r$, etiam potestas $(a \pm \alpha p)^m$ residuum relinquet $= r$.

Coroll. 1.

62. Si m sit 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 sit numerus impar, quia formula $-a^m$ per p diuisa residuum relinquit $= -r$, etiam formula $(\alpha p - a)^m$ residuum relinquet $= -r$.

Theorema 17.

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

Demonstratio.

Cum sit $a = c^n \pm \alpha p$, potestas $a^{\frac{p-1}{n}}$, seu $(c^n \pm \alpha p)^{\frac{p-1}{n}}$ 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 vnitatem relinquit, ergo etiam potestas $a^{\frac{p-1}{n}}$ vnitatem relinquet, siquidem sit $a = c^n \pm \alpha p$, 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 diuidantur, vnitatem relinquunt.

Coroll. 2.

66. Si ergo sit $a = cc \pm \alpha p$, existente p numero primo, tum potestas $a^{\frac{p-1}{2}}$ per p diuisa vnitatem 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 $a = c^3 \pm \alpha p$, tum potestas $a^{\frac{p-1}{3}}$ per p diuisa vnitatem 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, vt $p-1$ per 3 sit diuisibile.

Theorema 18.

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

Demonstratio.

Potestas $(c^n \pm \alpha p)^{\frac{p-1}{n}}$, 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 vnitatem relinquit, ergo et potestas $a^{\frac{p-1}{n}} b^{p-1}$. Huius autem factor b^{p-1} pariter vnitatem relinquit; ergo necesse est, alterum quoque factorem $a^{\frac{p-1}{n}}$, si per p diuidatur, vnitatem relinquere, nisi sit b vel c diuisibile per p.

Coroll. 1.

69. Si ergo sit $ab^n = c^n \pm \alpha p$, 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 vnitatem relinquant, 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 $a^m x^{mn} - y^{mn} = (ax^n - y^n)(a^{m-1}x^{mn-n} + a^{m-2}x^{mn-2n}y^n + a^{m-3}x^{mn-3n}y^{2n} + \ldots + y^{mn-n})$ 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

$$A = a^{m-1}x^{mn-n} + a^{m-2}x^{mn-2n} + \quad + 1$$
$$B = a^{m-1}x^{mn-n} + a^{m-2}x^{mn-2n}2^n + \ . \ . \ . \ + 2^{mn-n}$$
$$C = a^{m-1}x^{mn-n} + a^{m-2}x^{mn-2n}3^n + \ . \ . \ . \ + 3^{mn-n}$$
$$\vdots$$
$$N = a^{m-1}x^{mn-n} + a^{m-2}x^{mn-2n}(mn)^n + \ . \ . \ . \ + (mn)^{mn-n}$$

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 vti conſtat:

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

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 diviſibiles, neceſſario alter factor $ax^n - y^n$ per p erit diviſibilis,

Corol-

Corollarium 1.

73. Quicunque 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 quicunque 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 quicunque 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 ſit diui-

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 vndeuiceſimum, quod inuerſum eſt theorematis duodeuiceſimi, iam alibi propoſueram, ſed ſine demonſtratione, et tametſi tum eius demonſtrationem multis modis tentaui, eam tamen inuenire non potui, donec in methodum hic vſitatam incidi:

quae igitur eo magis notatu digna videtur, cum dubium sit nullum, quin eadem ad multa alia numerorum arcana viam sit patefactura. Haec quoque methodus, quae in consideratione differentiarum continetur, nuper mihi insigni vsui 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.