E262



# 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

$$1;\ a;\ a^2;\ a^3;\ a^4;\ a^5;\ a^6;\ a^7;\ a^8;\ \text{etc.}$$

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 $a^\mu$ et $a^\nu$ 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 $a^\mu$ det residuum $r$, potestas vero $a^\nu$ residuum $s$, fueritque $r + s = p$, 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 $a^\mu$ per $p$ diuisa praebeat residuum $r$, et potestas $a^\nu$ 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 $a^{\mu}$ 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 $a^{\mu}$ per $p$ diuiſae reſiduum ſit $= r$, fore poteſtatis $a^{2\mu}$ reſiduum $= rr$, poteſtatis $a^{3\mu}$ reſiduum $= r^3$; etc. Ita ſi poteſtatis $a^{\mu}$ 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 $a^{\mu}$ 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 $a^{4\mu}$ iterum $=+1$. Atque in genere poteſtatis $a^{n\mu}$ 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 | |
|---|---|---|
| $7^1$ | 7 | nempe cum poteſtas prima 7 relinquat 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.

 innu-

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 $a^{\mu}$ et $a^{\nu}$ 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 $a^{2}$ 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 $a^{\lambda}$ 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 $a^{\lambda}$, 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 $a^\lambda$ residuum $= 1$ praebentem, cuius exponens $\lambda$ 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 $a^\mu$ et $a^\nu$ 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 $a^\mu$ per $p$ diuisa, residuum relinquat $= r$, et potestatis altioris $a^{\mu+\nu}$ residuum sit $= rs$, erit potestatis $a^\nu$, qua haec illam superat, residuum $= s$.

## Demonstratio.

Praebeat enim potestas $a^\nu$ aliud residuum, puta $= t$, et cum potestatis $a^\mu$ 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 $a^\mu$ residuum sit $=r$, et potestatis $a^{\mu+\nu}$ residuum $=rs$, hinc sequitur potestatis $a^\nu$ residuum fore $=s$.

## Coroll. 1.

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

## Coroll. 2.

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

## Scholion.

19. Demonstratio huius theorematis etiam hoc modo confici potest. Cum $a^\mu$ 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 $a^\mu$ per $p$ non est diuisibilis. Ergo alter $a^\nu-s$ erit per $p$ diuisibilis, consequenter potestas $a^\nu$ per $p$ diuisa residuum dabit $=s$.

Theo-

## Theorema 5.

20. Si post vnitatem $a^{\lambda}$ 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 $a^{\mu}$, si per $p$ diuidatur, residuum quoque dare $=1$, et cum sit $\mu > \lambda$, neque tamen multiplo cuipiam ipsius $\lambda$ aequetur, hic exponens $\mu$ 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 $a^{\delta}$ vnitatem pro residuo habebit, foretque ergo $a^{\lambda}$ non minima potestas huius indolis contra hypothesin. Quare si $a^{\lambda}$ sit minima potestas residuum $=1$ praebens, nullae aliae potestates eadem proprietate erunt praeditae, nisi quarum exponentes sunt multipla ipsius $\lambda$.

## 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

quorum exponentes ſunt pares, omnes reſiduum habebunt idem $= 1$, reliqui vero termini, niſi $a^r$ 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

$= +1$,

$=+1$, tum poteſtas $a^n$ reſiduum dabit $=-1$. Ergo ſi minimae poteſtatis $a^\lambda$ reſiduum $=1$ praebentis exponens $\lambda$ 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 $a^\lambda$ reſiduum $1$ praebentis exponens $\lambda$ ſit numerus impar, tum nulla omnino poteſtas reſiduum relinquet $=-1$. Si enim quaepiam poteſtas, vti $a^\mu$, daret reſiduum $=-1$, tum poteſtas $a^{2\mu}$ daret reſiduum $=+1$, foretque idcirco $2\mu=n\lambda$, et quia $\lambda$ eſt numerus impar, foret $2\mu=2m\lambda$, ideoque $\mu=m\lambda$. At poteſtas $a^{m\lambda}$ relinquit reſiduum $=+1$, neque ergo reſiduum $-1$ vsquam occurrere poteſt.

## Theorema 7.

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

## Demonſtratio.

Si enim duae poteſtates, veluti $a^\mu$ et $a^\nu$, quarum exponentes $\mu$ et $\nu$ ſint minores, quam $\lambda$, 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

 hypo-

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

## Theorema. 8.

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

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

ita vt quoduis membrum $\lambda$ 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 $= 1$. 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 $a^1$ 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 $a^\mu$ 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 $a^\mu$.

## Coroll. 3.

31. Hic autem numerus $\mu$ minor quam $\lambda$ inuenitur, si numerus $x$ per $\lambda$ diuidatur, tum enim residuum, quod in hac diuisione remanet, erit hic ipse numerus $\mu$, qui quaeritur.

## Coroll. 4.

32. Semper autem datur potestas $a^\lambda$, quae per $p$ diuisa vnitatem relinquit, cuius exponens $\lambda$ 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 $a^\lambda$ sit minima earum, quae per numerum $p$ diuisae vnitatem relinquunt; tunc

 quia

quia finguli termini minores quam $a^\lambda$ diuerfa praebent refidua, in refiduis omnibus, neque plures, neque pauciores diuerfi numeri occurrent quam $\lambda$. Igitur fi $\lambda$ fit minus quam $p-1$, non omnes numeri in refiduis occurrent: fed quidam numeri plane nunquam in diuifione terminorum progreffionis geometricae $1, a, a^2, a^3$ etc. remanere poterunt.

## Coroll. 6.

34. Si igitur diuerfitas refiduorum fpectetur, fieri poteft, vt ex omnibus poteftatibus ipfius $a$ vnicum tantum refiduum, vel duo tantum refidua diuerfa, vel tria etc. prodeant, plura tamen nunquam quam $p-1$ locum habere poffunt. Quotquot autem prodierint refidua, inter ea femper vnitas reperitur.

## Theorema 9.

35. Si $p$ fit numerus primus, et $a$ primus ad $p$, atque omnes numeri ipfo $p$ minores reperiantur inter refidua, quae ex diuifione omnium poteftatum ipfius $a$ per numerum primum $p$ oriuntur, tum $a^{p-1}$ erit minima poteftas, quae per $p$ diuifa vnitatem relinquit.

## Demonftratio.

Sit $a^\lambda$ minima poteftas, quae per $p$ diuifa relinquat vnitatem, atque ex praecedentibus patet, effe $\lambda < p$ (15). Iam cum numerus omnium refiduorum diuerforum fit $=\lambda$, et omnium numerorum ipfo $p$ minorum $=p-1$, patet, fi effet $\lambda < p-1$, 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 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 $a^{\mu}$ daret residuum $r$, quod esset pars aliquota ipsius $p$, ob $a^{\mu} = mp + r$, etiam ipsa potestas $a^{\mu}$ 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 $a^{\lambda}$ 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 $a^\alpha$ 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 $a^\mu$ 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 $a^\nu k$, convenirent, 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 $\lambda$ numeri, qui in residuis locum non inueniunt, siquidem sit $\lambda < p - 1$.

## Coroll. 1.

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

## Coroll. 2.

39. Si ergo $a^\lambda$ 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 $\lambda$ 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 $\lambda$.

## Theorema 2.

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

## Demonſtratio.

Cum $a^\lambda$ ſit minima poteſtas, quae per numerum primum $p$ diuiſa, vnitatem relinquit, plures in reſiduis non occurrunt numeri diuerſi, quam $\lambda$, 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 $\lambda$ 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 diverſi.

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 $\lambda$ numeri, qui non sunt residua, sique cum $\lambda$ habeamus residua, et $2\lambda$ non-residua, hique numeri omnes sint ipso $p$ minores, fieri nequit, vt sit eorum summa $3\lambda$ 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 $a^{\lambda}$ vnitatem relinquat, etiam $a^{2\lambda}$ et $a^{3\lambda}$ vnitatem pro residuo dabunt.

## Theorema 12.

44. Si $a^{\lambda}$ sit minima potestas ipsius $a$, quae per numerum primum $p$ diuisa vnitatem relinquit, fueritque

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

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

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

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

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

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 $\lambda$: ſi enim plures fuerint iſtiusmodi numeri quam $n\lambda$, tum ob vnicum ſtatim $\lambda$ noui inſuper accedunt, vt eorum omnium numerus fiat $=(n+1)\lambda$; at ſi hic nondum omnes numeri non-reſidua contineantur, denuo ſubito $\lambda$ noui accedent.

## Theorema 13.

48. Si $p$ ſit numerus primus, et $a^{\lambda}$ minima poteſtas ipſius $a$, quae per $p$ diuiſa vnitatem relinquit, erit exponens $\lambda$ diuiſor numeri $p-1$.

## Demonſtratio.

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

 mino-

minorum, qui residua esse nequeunt, erit $= p - 1 - \lambda$, at hic numerus (47) est multiplum ipsius $\lambda$, puta $n\lambda$, ita vt sit $p - 1 - \lambda = n\lambda$, vnde fit $\lambda = \frac{p-1}{n+1}$. Perspicuum ergo est, exponentem $\lambda$ esse diuisorem numeri $p - 1$, vnde si non sit $\lambda = p - 1$, certe parti cuidam aliquotae numeri $p - 1$ exponens $\lambda$ 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 $a^{\lambda}$ minima potestas ipsius $a$, quae per $p$ diuisa vnitatem relinquit, erit, vt vidimus, $\lambda < p$, atque insuper demonstrauimus, esse vel $\lambda = p - 1$, vel $\lambda$ esse partem aliquotam numeri $p - 1$. Priori casu constat propositum, atque potestas $a^{p-1}$ per $p$ diuisa vnitatem relinquet. Posteriori casu, quo $\lambda$ est pars aliquota numeri $p - 1$, erit $p - 1 = n\lambda$, at cum potestas $a^{\lambda}$ 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 eueniet. 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 $\lambda$ 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 $p$ diviſus vnitatem relinquat.

## Demonſtratio.

Sit enim $a^\lambda$ 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 ſit 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 $(-a + \alpha p)^m$, 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 $ab^n = c^n + \alpha p$, 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 $(c^n + \alpha p)^{\frac{p-1}{n}}$, seu $a^{\frac{p-1}{n}} b^{p-1}$, per $p$ diuisa idem relinquit residuum, quod potestas $c^{n.\frac{p-1}{n}} = c^{p-1}$, 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

$A = a$

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

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:

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

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

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.

SPECI-