1763

Theoremata arithmetica nova methodo demonstrata

Leonhard Euler

THEOREMATA ARITHMETICA NOVA METHODO DEMONSTRATA.

Auctore

L. EVLERO.

Praeter varias computandi operationes, quae vulgo in Arithmetica tradi solent, huiusque disciplinae quasi partem practicam constituunt, eiusdem pars Theoretica, quae in indaganda numerorum natura versatur, non minus iam olim tractari est coepta, quemadmodum ex *Euclide* et *Diophanto* intelligere licet, vbi insignes numerorum proprietates erutae reperiuntur ac demonstratae. Quo magis autem deinceps numerorum indolem et affectiones Mathematici sunt scrutati, multo plures eorum proprietates obseruauerunt, vnde pulcherrima Theoremata numerorum naturam illustrantia deriuauere, quae partim demonstrationibus sunt munita, partim etiam nunc iis indigent, siue quod eae ab auctoribus non sint inuentae, siue temporum iniuria deperditae: ex quo genere plurima passim occurrunt huiusmodi Theoremata numerica, quorum demonstrationes adhuc desiderantur, etiamsi eorum veritatem in dubium vocare non liceat. Atque hic insigne discrimen, quod inter Theoremata arithmetica et geometrica intercedit, non parum mirari debemus, quod vix vlla propositio geometrica proferri possit, quam non sit in promtu, siue veram, siue falsam, ostendere, dum

dum contra multae circa numerorum naturam notae sunt propositiones, quarum veritatem nobis agnoscere, neutiquam vero demonstrare liceat. Magna huiusmodi Theorematum copia a *Fermatio* relicta habetur, quorum demonstrationes maximam partem se inuenisse affirmauit, quas cum eius scriptis interiisse in eximium huius scientiae detrimentum non parum est dolendum. Quot autem talium Theorematum demonstrationes vel sunt cognitae, vel restitutae, in iis certe multo maior vis ingenii elucet, quam vix in vllo alio demonstrationum genere deprehendimus; vnde in hoc negotio non tam vtilitas, qua scientia numerorum illustratur, est aestimanda, quam maxima subtilitas, qua huiusmodi demonstrationes prae aliis distinguuntur. Atque ob hanc causam, cum iam saepius, quam plerisque aequum videri queat, in hoc genere laborauerim, operam mihi equidem non perdidisse videor, neque etiam nunc theoremata, quae hic propono, vtilitate caritura confido. Notatu imprimis dignum visum est Theorema illud *Fermatii*, quo omnes numeros in hac formula $a^{p-1}-1$ contentos, semper diuisibiles esse per numerum p, siquidem is fuerit primus, neque tamen a per eum diuisionem admittat, affirmauit, cuius Theorematis iam geminam dedi demonstrationem. Nunc autem idem in latiori sensu contemplor, atque in genere, si diuisor non sit numerus primus, sed quicunque N, inuestigo, cuiusmodi exponentem potestati cuicunque tribui oporteat, vt expressio a^n-1 semper sit diuisibilis per numerum N, dummodo numerus a cum eo nullum habeat diuisorem communem. Inueni au-

tem hoc semper vsu venire, quoties exponens n aequalis fuerit multitudini numerorum ipso N minorum, qui sint ad N primi. Ad hoc ergo demonstrandum, ante omnia huiusmodi theorematibus est opus, ex quibus, proposito numero quocunque N, cognosci possit, quot inter numeros ipso minores futuri sint ad eum primi, seu qui nullum cum eo habeant communem diuisorem; quae theoremata iam ipsa, multo ampliorem vsum habere, atque ad alias magis absconditas numerorum proprietates aditum parere, videntur. Iis autem praemissis, demonstratio veritatis propositae ita est comparata, vt maiore attentione non indigna videatur.

Theorema 1.

1. Si per numerum quemcunque n termini progressionis arithmeticae cuiuscunque, cuius differentia sit numerus ad n primus, diuidantur, inter residua occurrent omnes numeri diuisore n minores.

Demonstratio.

Sit progressionis arithmeticae terminus primus $= a$, et differentia $= d$, quae sit ad n numerus primus, seu quae cum numero n nullum praeter vnitatem habeat diuisorem communem, ita vt progressio arithmetica futura sit:

$$a, a + d, a + 2d, a + 3d, a + 4d, a + 5d, \text{ etc.}$$

ac dico: si singuli termini per numerum n diuidantur, inter residua omnes numeros ipso n minores occurrere.

Ad

Ad hoc demonstrandum sufficiet huius progressionis tantum n terminos considerasse, qui sunt:

$$a, a+d, a+2d, a+3d, \ldots a+(n-1)d.$$

Quodsi ergo isti termini singuli per n diuidantur, omnia residua inter se diuersa esse oportet. Si enim duo termini, veluti $a+\mu d$ et $a+\nu d$, existentibus μ et ν numeris ipso n minoribus, per n diuisi paria praeberent residua, eorum differentia $(\nu-\mu)d$ vtique per n esset diuisibilis. Cum autem numeri d et n nullum habeant diuisorem communem, necesse esset, vt $\nu-\mu$ diuisionem per n admitteret; id quod esset absurdum, ob $\nu-\mu<n$. Quare cum omnia illa residua sint diuersa, eorumque numerus, vtpote terminorum numero aequalis, sit $=n$, in iis omnes plane numeri ipso n minores occurrent, scilicet:

$$0, 1, 2, 3, 4, 5, \ldots\ldots (n-1)$$

siquidem differentia progressionis d sit numerus ad diuisorem propositum n primus. Q. E. D.

Coroll. 1.

2. Inter terminos ergo progressionis arithmeticae cuiuscunque, quorum numerus est n, dummodo differentia eius ad n sit numerus primus, certe reperitur vnus, qui per n est diuisibilis: tum vero etiam aderit vnus, qui per n diuisus datum residuum r relinquit.

Coroll. 2.

3. Si ergo numerus d ad n fuerit primus, semper numerus huius formae $a+\nu d$ exhiberi potest,

existente a numero quocunque et ν minore quam n, qui per numerum n sit diuisibilis, atque etiam sub iisdem conditionibus semper talis dabitur numerus $a+\nu b$, qui per n diuisus datum relinquat residuum r.

Coroll. 3.

4. Datis igitur numeris a et d, quorum hic d ad n sit primus, semper inuenire licet numeros μ et ν, vt aequationi huic: $a+\nu d=\mu n$, vel etiam huic: $a+\nu d=\mu n+r$ satisfiat, quicunque numerus minor quam n pro r assumatur.

Scholion.

5. Quod de progressionis arithmeticae terminorum numero n demonstrauimus, id de tota progressione in infinitum continuata valet: termini enim, qui post illos n terminos sequuntur, eadem ordine reproducunt residua, si per n diuidantur. Ita terminorum post $a+(n-1)d$ sequentium, qui sunt $a+nd$, $a+(n+1)d$; $a+(n+2)d$ etc. per n diuisorum residua, conueniunt cum residuis ex terminis initialibus a, $a+d$, $a+2d$, etc. natis. Atque si tota series in infinitas periodos distribuatur, cuique n terminos tribuendo, hoc modo:

$$a,a+b\ldots,a+(n-1)b|a+nb\ldots a+(2n-1)b|a+2nb\ldots a+(n-1)b|$$

termini cuiuslibet periodi eadem praebebunt residua, eodemque ordine dispositа; omnium enim periodorum termini cum primi, tum secundi, et tertii etc. constanter paria dabunt residua. Quare si rationem residuorum

duorum cognoſcere velimus, ſufficit vnicam periodum examinaſſe.

Theorema 2.

6. In progreſſione arithmetica, cuius terminorum numerus eſt $= n$, totidem termini erunt ad numerum n primi, quot inter numeros ipſo n minores dantur ad n primi, dummodo differentia progreſſionis fuerit ad n numerus primus.

Demonſtratio.

Sit enim a terminus primus, et d differentia progreſſionis, quae ſit ad n numerus primus, ideoque ipſa progreſſio n continens terminos:

$$a, a+d, a+2d, a+3d, \ldots\ldots a+(n-1)d.$$

Quoniam igitur, ſi hi termini per numerum n diuidantur, inter reſidua occurrunt omnes plane numeri ipſo n minores; ponamus ex termino quocunque $a+\nu d$ reſultare reſiduum r, ac manifeſtum eſt, ſi r fuerit numerus ad n primus, illum quoque terminum $a+\nu d$ ad n fore primum, ſin autem r cum n habeat quempiam diuiſorem communem, idem quoque erit diuiſor communis numerorum n et $a+\nu d$. Quare quot inter numeros ipſo n minores fuerint numeri ad n primi, totidem quoque inter terminos progreſſionis arithmeticae propoſitae habebuntur numeri ad n primi. Q. E. D.

Coroll. 1.

7. Si n fuerit numerus primus, quia omnes numeri, ipſo minores, ad ipſum quoque ſunt primi, quorum

quorum numerus ergo est aequalis $=n-1$; in illa etiam progressione arithmetica omnes termini praeter vnum erunt ad n primi; quippe vnus per n est diuisibilis.

Coroll. 2.

8. Sin autem n fuerit numerus compositus, inter numeros ipso minores dabuntur quipiam, qui cum eo diuisorem habeant communem; totidemque vero etiam reperientur in progressione arithmetica, quibus iidem communes diuisores cum n conueniant.

Coroll. 3.

9. Ita si sit $n=6$, quia inter numeros senario minores sunt duo ad 6 primi, scilicet 1 et 5; in omni progressione arithmetica 6 terminorum:

$$a, a+d, a+2d, a+3d, a+4d, a+5d$$

duo tantum erunt ad 6 primi, dummodo differentia d sit ad 6 numerus primus. Ita si capiatur $a=4$; $d=5$, horum sex numerorum 4, 9, 14, 19, 24, 29, duo, scilicet 19 et 29, ad 6 sunt primi, vnus 24 per 6 diuisibilis, reliqui vero 4, 9, 14 ad 6 compositi perinde ac 2, 3, 4.

Scholion.

10. Haec Theoremata in doctrina et contemplatione naturae numerorum insignem habent vsum, hic autem ea solum adhibere visum est ad hanc quaestionem enodandam: *Proposito numero quocunque* n, *quot inter numeros ipso minores futuri sint ad eundem numerum*

rum n *primi*? Statim quidem patet si n sit numerus primus, omnes numeros ipso minores simul ad eum fore primos, eorumque idcirco numerum esse $=n-1$. Verum si n sit numerus compositus, multitudo numerorum ipso minorum ad eumque primorum est minor, quanta autem sit quouis casu, non tam facile assignari potest. Ita, si sit $n=12$, inter numeros minores tantum quatuor reperiuntur ad 12 primi, scilicet 1, 5, 7, 11: et si sit $n=60$, numeri minores ad eum primi sunt:

1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59

quorum numerus est 16: vnde reliqui 43 omnes cum 60 diuisores habent communes. Moneri hic conuenit, vnitatem ad omnes plane numeros esse numerum primum, etiamsi omnium sit diuisor; id quod ex definitione est euidens, qua numeri dicuntur esse inter se primi, qui praeter vnitatem alium nullum agnoscunt diuisorem.

Theorema 3.

11. Si n sit potestas quaecunque numeri primi p, seu $n=p^m$, inter numeros ipso minores tot erunt ad eum primi, quot vnitates continentur in $p^m-p^{m-1}=p^{m-1}(p-1)$.

Demonstratio.

Multitudo omnium numerorum potestate $n=p^m$ minorum est p^m-1, inter hos autem reperiuntur quidam, qui ad n non sunt primi, omnia scilicet ipsius p multipla, minora quam n, nullique alii praeterea: ex quo sequentes numeri ad n non erunt primi:

$$p, 2p, 3p, 4p - - - - - - - p^m-p$$

quorum numerus est $p^{m-1}-1$; quo ablato a numero omnium ipso $n=p^m$ minorum, relinquitur multitudo eorum, qui ad p^m sunt primi, quorum numerus itaque est $=p^m-p^{m-1}=p^{m-1}(p-1)$. Q. E. D.

Coroll. 1.

12. Hinc igitur primo sequitur, id quod per se est manifestum, si sit $n=p$, existente p numero primo, numerum omnium numerorum ipso minorum ad eumque primorum esse $=p-1$, siquidem omnes numeri ipso minores simul sunt ad eum primi.

Coroll. 2.

13. At si sit $n=p^2$, inter numeros ipso minores, multitudo eorum, qui ad eum sunt primi, est $=pp-p=p(p-1)$; reliqui, quorum numerus est $p-1$, ad $n=p^2$ erunt compositi, seu per p diuisibiles.

Coroll. 3.

14. Proposita autem numeri primi potestate quacunque $n=p^m$, inter numeros ipso minores, quorum multitudo est $=p^m-1$, reperiuntur $p^{m-1}-1$, qui sunt per p diuisibiles, ideoque ad p^m non primi: reliqui vero omnes, quorum numerus est $=p^m-p^{m-1}=p^{m-1}(p-1)$ ad p^m sunt primi.

Scholion.

15. Si ergo numerus propositus n fuerit potestas cuiuspiam numeri primi, ope huius regulae assignare pote-

poterimus, quot inter omnes numeros ipſo minores futuri ſint ad eum primi. Quando autem numerus n, ex duobus pluribusue numeris primis fuerit conflatus, hinc nondum iſta quaeſtio confici poteſt: praecedentibus autem Theorematibus adhibendis iſtam quaeſtionem latius patentem reſoluere poterimus.

Theorema 4.

16. Si numerus n ſit productum duorum numerorum primorum p et q, ſeu $n = pq$, multitudo omnium numerorum ipſo minorum ad eumque primorum eſt $= (p-1)(q-1)$.

Demonſtratio.

Cum numerus omnium numerorum ipſo $n = pq$ minorum ſit $pq-1$, hinc primum ii debent excludi, qui per p ſunt diuiſibiles, deinde vero etiam ii, qui per q, hisque deletis relinquetur multitudo quaeſita. Notentur ergo ab vnitate vsque ad pq numeri, qui ſunt ad p primi, hoc modo:

1,	2,	3,	4,	- -	$p-1$
$p+1$,	$p+2$,	$p+3$,	$p+4$	- -	$2p-1$
$2p+1$,	$2p+2$,	$2p+3$,	$2p+4$	- -	$3p-1$
$3p+1$,	$3p+2$,	$3p+3$,	$3p+4$	- -	$4p-1$
:	:	:	:		:
:	:	:	:		:
:	:	:	:		:
$(q-1)p+1$,	$(q-1)p+2$,	$(q-1)p+3$,	$(q-1)p+4$	- -	$pq-1$

atque iam ex his ii tantum eligi debent, qui ſimul

quoque ad q sunt primi. Considerentur ergo series verticales, quarum numerus est $p-1$; quaelibet autem continet q terminos in arithmetica progressione crescentes, differentia existente p, quae est ad q numerus primus. In qualibet ergo serie verticali omnes termini praeter vnum ad q erunt primi (per §. 7.); vnde vnaquaeque series verticalis continet $q-1$ numeros ad q primos. Quare cum numerus serierum verticalium sit $p-1$, in omnibus continentur simul $(p-1)(q-1)$ numeri ad q primi, iidemque igitur etiam ad productum pq erunt primi; consequenter inter omnes numeros ipso pq minores reperientur $(p-1)(q-1)$ numeri ad pq primi. Q. E. D.

Coroll. 1.

17. Cum multitudo omnium numerorum ipso producto pq minorum sit $pq-1$, inter eos semper sunt $(p-1)(q-1)=pq-p-q+1$ primi ad pq, reliqui vero, quorum numerus est $p+q-2$, ad eum sunt compositi, seu cum eo communem habent diuisorem vel p, vel q.

Coroll. 2.

18. Hoc etiam inde patet, quod inter numeros ipso producto pq minores sint $q-1$ numeri per p diuisibiles, scilicet:

$$p, 2p, 3p, 4p \ldots\ldots\ldots (q-1)p$$

deinde inter eosdem sunt $p-1$ numeri per q diuisibiles, nempe:

$$q, 2q, 3q, 4q \ldots\ldots\ldots (p-1)q$$

qui cum ab illis omnes sint diuersi, omnino habentur

$(q-1)$

$(q-1)+(p-1)=p+q-2$ numeri, qui ad pq non sunt primi.

Coroll. 3.

19. Si ergo quaeratur, quot ab 1 vsque ad 15 sint numeri ad 15 primi? ob $p=3$ et $q=5$, regula docet eorum numerum esse $2.4=8$, quippe qui sunt 1, 2, 4, 7, 8, 11, 13, 14. Simili modo ab 1 ad 35 ob $p=5$ et $q=7$, multitudo numerorum ad 35 primorum est $4.6=24$, hique numeri sunt: 1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34.

Scholion.

20. Quoniam hic quaestio est de numeris, qui ad quempiam numerum sint primi, eoque minores, eos commode partes ad istum numerum primas appellare licebit. Ita si numerus propositus fuerit primus $=p$, numerus partium ad eum primarum est $=p-1$: si numerus propositus sit potestas quaecunque numeri primi $=p^n$, numerus partium ad eum primarum erit $=p^n-p^{n-1}=p^{n-1}(p-1)$: at si numerus propositus sit productum duorum numerorum minorum disparium $=pq$, numerus partium ad eum primarum est $=(p-1)(q-1)$, hocque modo ambages in loquendo contrahemus. Simili modo demonstrare possemus, si numerus propositus sit productum ex tribus numeris primis disparibus $=pqr$, numerum partium ad eum primarum fore $=(p-1)(q-1)(r-1)$: hocque adeo ad productum plurium extendere liceret. Verum sequens propositio omnes hos casus in se complectetur.

Theorema 5.

21. Si ſint A et B numeri inter ſe primi, et numerus partium ad A primarum ſit $=a$, numerus vero partium ad B primarum ſit $=b$; tum numerus partium ad productum AB primarum erit $=ab$.

Demonſtratio.

Sint $1, \alpha, \beta, \gamma, \ldots\ldots \omega$ numeri illi ipſo A minores ad eumque primi, ſeu partes ad A primae, quarum igitur partium numerus per hypotheſin eſt $=a$. Totidem ergo erunt numeri ad A, itidem primi erunt ab A ad 2A, item a2A ad 3A, et ita porro. Hoc modo exhiberi poterunt omnes numeri ad A primi ab vnitate vsque ad numerum propoſitum AB, quos ſequens ſchema exhibebit:

$1,$	$\alpha,$	$\beta,$	$\ldots\ldots$	ω
$A+1,$	$A+\alpha,$	$A+\beta$	$\ldots\ldots$	$A+\omega$
$2A+1,$	$2A+\alpha,$	$2A+\beta$	$\ldots\ldots$	$2A+\omega$
$3A+1,$	$3A+\alpha,$	$3A+\beta$	$\ldots\ldots$	$3A+\omega$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
$(B-1)A+1,$	$(B-1)A+\alpha,$	$(B-1)A+\beta,$	$\ldots$	$(B-1)A+\omega.$

Hic ſingulae ſeries horizontales continent a terminos, numerusque omnium ſerierum horizontalium eſt $=B$; vnde omnes ſeries iunctim offerunt aB terminos, qui iam omnes ad A erunt primi. Inde ergo adhuc excludi debent ii, qui ad B non ſunt primi, vt hoc modo relinquantur, qui non ſolum ad A, ſed etiam ad B, ideoque ad ipſum productum AB, ſint primi, ſeu ex

ex his seriebus ii tantum termini numerari debent, qui etiam ad B sint primi. Hunc in finem consideremus series verticaliter; et cum numerus serierum verticalium sit $= a$, quaelibet series verticalis continebit B terminos in arithmetica progressione auctos, quorum differentia cum sit $=$ A, ideoque numerus ad B primus, per Theor. II. quaelibet series verticalis tot continebit terminos ad B primos, quot dantur partes ad numerum B primae; eorum ergo numerus est per hypothesin $= b$. Cum igitur singulae series verticales contineant b terminos ad B primos, qui propterea etiam erunt ad productum AB primi; numerus omnium terminorum ad AB primorum, hoc est partium ad hunc numerum AB primarum erit $= ab$. Q. E. D.

Coroll. 1.

22. Si insuper tertius numerus C adiiciatur, qui sit ad vtrumque praecedentium A et B, seu ad eorum productum AB primus, et numerus partium ad C primarum sit $= c$; tum numerus partium ad productum ABC primarum erit $= abc$. Productum enim AB considerari potest tanquam vnus numerus, cuius partium ad eum primarum sit $= ab$; et quia C ad AB est primus, Theorema hic habet locum.

Coroll. 2.

23. Cum igitur vnusquisque numerus N resolui possit in factores inter se primos, qui singuli sint vel ipsi numeri primi, vel potestates primorum, ope huius regulae multitudo partium ad numerum quemcunque N primarum assignari poterit.

Coroll. 3.

Coroll. 3.

24. Exiſtentibus ſcilicet p, q, r, s, etc. numeris primis, omnis numerus N in huiusmodi forma $N = p^{\lambda} q^{\mu}, r^{\nu}, s^{\xi}$ comprehendetur; vnde numerus partium ad N primarum erit:

$$p^{\lambda-1}(p-1).\ q^{\mu-1}(q-1).\ r^{\nu-1}(r-1).\ s^{\xi-1}(s-1).$$

Coroll. 4.

25. Pro formis igitur numerorum ſimplicioribus multitudo partium ad eos primarum ita ſe habebit:

numerus propoſitus	multitudo partium ad eum primarum	num. prop.	mult. part. ad eum prim.
p	$p-1$	2	1
pp	$p(p-1)$	3	2
pq	$(p-1)(q-1)$	4	2
p^3	$pp(p-1)$	5	4
p^2q	$p(p-1)(q-1)$	6	2
pqr	$(p-1)(q-1)(r-1)$	7	6
p^4	$p^3(p-1)$	8	4
p^3q	$p^2(p-1)(q-1)$	9	6
p^2q^2	$p(p-1)q(q-1)$	10	4
p^2qr	$p(p-1)(q-1)(r-1)$	11	10
$pqrs$	$(p-1)(q-1)(r-1)(s-1)$	12	4
p^5	$p^4(p-1)$	13	12
p^4q	$p^3(p-1)(q-1)$	14	6
p^3q^2	$p^2(p-1)q(q-1)$	15	8
p^3qr	$p^2(p-1)(q-1)(r-1)$	16	8
p^2q^2r	$p(p-1)q(q-1)(r-1)$	17	16
p^2qrs	$p(p-1)(q-1)(r-1)(s-1)$	18	6
$pqrst$	$(p-1)(q-1)(r-1)(s-1)(t-1)$	19	18
		20	8
		21	12
		22	10
		23	22
		24	8
		25	20

Coroll.

Coroll. 5.

26. Hinc igitur propoſito numero quocunque multitudo partium ad eum primarum expedite definietur. Veluti, ſi proponatur 360, cum ſit $360 = 2^3 \cdot 3^2 \cdot 5$, erit multitudo partium ad 360 primarum $= 4.6.4 = 96$.

Scholion.

27. Haec circa multitudinem partium ad numerum quemuis primarum pro praeſenti inſtituto ſufficere poſſunt. Interim tamen circa ipſas partes ad quemuis numerum primas haec notaſſe iuuabit: ſi numerus propoſitus fuerit N, atque inter partes ad eum primas occurrat numerus α, ibidem quoque occurret numerus $N-\alpha$; quoniam, exiſtente α ad N primo, etiam $N-\alpha$ erit ad N primus. Hinc pro quouis numero partes tantum eius ſemiſſe minores inueniſſe ſufficiet, cum reliquae ſint earum complementa ad ipſum numerum N. Simili modo, ſi N ſit numerus par, inter partes ad N primas etiam occurret $\frac{1}{2}N-\alpha$, tum etiam $\frac{1}{2}N+\alpha$. Item ſi N ſit diuiſibilis per numerum quemcunque n, inter partes ad eum primas quoque occurrent hi numeri:

$\frac{1}{n}N \pm \alpha$; $\frac{2}{n}N \pm \alpha$; $\frac{3}{n}N \pm \alpha$ .... $\frac{(n-1)}{n}N \pm \alpha$, et $N-\alpha$ hincque multo facilius ipſae partes iſtae actu exhiberi poterunt.

Theorema 6.

28. Si numerus x fuerit primus ad N, tum omnes poteſtates ipſius x per N diuiſae relinquent reſidua, quae erunt ad numerum N prima.

Demonſtratio.

Cum enim x ſit numerus ad N primus, omnes eius poteſtates erunt quoque ad N primae, ideoque ſi per N diuidantur, reſidua etiam ad N erunt numeri primi. Q. E. D.

Coroll. 1.

29. Inter reſidua ergo poteſtatum ipſius x per N diuiſarum alii numeri non occurrunt, niſi qui ſint partes ad N primae; quarum numerus cum ſit pro indole numeri N determinatus, innumerabiles exiſtent poteſtates ipſius x, quae per N diuiſae aequalia relinquunt reſidua.

Coroll. 2.

30. Inter reſidua autem iſta ex diuiſione poteſtatum ipſius x per numerum N orta ſemper reperietur vnitas, propterea quod inter poteſtates ipſius x etiam referri debet $x^0 = 1$. Vtrum autem praeter vnitatem etiam omnes reliquae partes ad N primae inter reſidua occurrant, nec ne? mox videbimus.

Coroll. 3.

31. Si pro x capiatur vnitas, omnia reſidua erunt vnitates, quicunque numerus pro N fuerit aſſumtus. Deinde ſi ſumatur $x = N - 1$, qui numerus ad N etiam eſt primus, in reſiduis, ex diuiſione poteſtatum $(N-1)^0$, $(N-1)^1$, $(N-1)^2$, $(N-1)^3$, etc. ortis, nonniſi duo reperientur diuerſa, ſcilicet 1 et $N-1$, quae continuo ſe alternatim excipiunt.

Coroll. 4.

Coroll. 4.

32. Prout igitur numerus x ratione ad N fuerit comparatus, vtique fieri potest, vt inter residua omnium potestatum ipsius x non omnes partes ad diuisorem N primae occurrant.

Coroll. 5.

33. Si ergo omnes partes ad numerum N primae sint $1, a, b, c, d, e, \ldots$ quarum numerus sit $= n$, inter residua memorata, vel omnes istae partes occurrent, vel quaedam tantum, inter quas autem semper vnitas reperietur.

Coroll. 6.

34. Quodsi non omnes illae partes in residuis ex diuisione potestatum ipsius x per numerum N relictis occurrant, illae partes in duas classes distribuentur, quarum altera continebit partes in residuis occurrentes, altera vero partes in residuis non occurrentes.

Theorema 7.

Si series potestatum $x^0, x^1, x^2, x^3, x^4 x^5$, etc. per numerum N, qui ad x sit primus, diuidatur, eousque residua prodibunt diuersa, donec perueniatur ad potestatem, quae iterum vnitatem pro residuo praebeat.

Demonstratio.

Quoniam serie potestatum $1, x, x^2, x^3, x^4$, etc. in infinitum continuata, omnia residua diuersa esse nequeunt, necesse est, vt tandem quodpiam ex praecedentibus

tibus reſiduis redeat; ac dico: vnitatem eſſe id reſiduum, quod omnium primum ſit rediturum. Quod ſi quis neget, ſit x^μ ea poteſtas, cuius reſiduum primum in ſequentibus ex poteſtate $x^{\mu+\nu}$ redeat; cum igitur poteſtates x^μ et $x^{\mu+\nu}$ aequalia praebeant reſidua, earum differentia $x^{\mu+\nu} - x^\mu = x^\mu(x^\nu - 1)$ per numerum N erit diuiſibilis. Verum producti $x^\mu(x^\nu - 1)$ factor prior ad N eſt numerus primus, ergo alter $x^\nu - 1$ per N diuiſibilis ſit neceſſe eſt. Hinc autem poteſtas x^ν per N. diuiſa reſiduum daret $= 1$, ſicque vnitas inter ſequentia redua citius redibit, quam reſiduum poteſtatis x^μ, quippe quod per hypotheſin demum in poteſtate altiore $x^{\mu+\nu}$ recurrit. Ex quo euidens, nullum reſiduum iterum occurrere poſſe, niſi ante vnitas inter reſidua redierit. Q. E. D.

Coroll. 1.

36. Poſtquam diuiſio terminorum ſeriei $1, x, x^2, x^3, x^4$, etc. per numerum N ad x primum ab initio dedit reſidua diuerſa, puta $1, \alpha, \beta, \gamma$ etc. tandem iterum occurret primum reſiduum 1; quod ſi oriatur ex poteſtate x^ν, numerus praecedentium reſiduorum diuerſorum erit $= \nu$.

Coroll. 2.

37. Quando autem poteſtas x^ν reſiduum dat 1, idem quod primus terminus x^0, poteſtas ſequens $x^{\nu+1}$ idem dabit reſiduum quod x^1; et ſequentium quaecunque $x^{\nu+\mu}$ idem quod poteſtas x^μ. Cum enim differentia

rentia $x^{\nu+\mu} - x^{\mu} = x^{\mu}(x^{\nu} - 1)$ fit diuiſibilis per N, neceſſe eſt, vt ambo termini $x^{\nu+\mu}$ et x^{μ} per N diuiſi idem praebeant reſiduum.

Coroll. 3.

38. Cum poſt poteſtatem x^{ν} eadem reſidua $1, \alpha, \beta, \gamma$ etc. ordine recurrant, poteſtas $x^{2\nu}$, ſimili-que modo poſt eam poteſtates $x^{3\nu}$, $x^{4\nu}$, $x^{5\nu}$ etc. omnes per N diuiſae idem reſiduum 1 relinquent. Quin etiam omnes poteſtates x^{μ}, $x^{\mu+\nu}$, $x^{\mu+2\nu}$, $x^{\mu+3\nu}$, $x^{\mu+4\nu}$ etc. aequalia reſidua ſuppeditabunt.

Coroll. 4.

39. Si igitur x^{ν} fuerit infima poteſtas, quae poſt $x^{0} = 1$ iterum vnitatem pro reſiduo praebeat, numerus diuerſorum reſiduorum erit ν. Cum ergo numerus partium ad numerum N primarum ſit $= n$, fieri certe nequit, vt ſit $\nu > n$: erit ergo vel $\nu = n$, vel $\nu < n$.

Coroll. 5.

40. Si ergo ſeries poteſtatum $1, x, x^{2}, x^{3}$, etc. vsque ad x^{n} continuetur, inter eas certe vna ſaltem reperietur praeter primum terminum 1, quae per N diuiſa vnitatem relinquat. Plures fortaſſe huiusmodi poteſtates aliquando, ſed pauciores vna nunquam exiſtent.

Scholion.

41. Reſidua proprie ſemper ſunt numeri minores diuiſore N, ſed nihil impedit, quo minus numeros

etiam maiores tanquam residua spectemus, cuiusmodi relinquuntur, si quotus nimis paruus accipiatur. Ita si in diuisione cuiuspiam numeri per N relinquatur $N+\alpha$, hoc residuum aequiualens ipsi α censeri debet; hincque, si de residuis sermo sit, omnes hi numeri α, $N+\alpha$, $2N+\alpha$, $3N+\alpha$, etc. instar vnius residui α sunt considerandi. Scilicet multipla quaecunque diuisoris N siue adiecta, siue demta a quopiam residuo α, eius naturam non mutant, atque hoc modo etiam numeri negatiui commode inter residua referuntur; veluti $\alpha-N$ pro eodem residuo est habendum ac α; et residuum -1 aequiualet residuo $N-1$. Ex his conficitur, omnes numeros, qui per N diuisi idem exhibeant residuum α, pro eodem residuo haberi posse, ex quo enim numero per diuisionem quotum nimis paruum sumendo oritur residuum vel $N+\alpha$, vel $2N+\alpha$, vel $3N+\alpha$ etc. ex eodem, quotum plenum sumendo, nascitur residuum α; tum vero indidem, si quotus capiatur nimis magnus, obtinebuntur residua negatiua $\alpha-N$, vel $\alpha-2N$, vel $\alpha-3N$ etc. quae ergo etiam ab α non discrepare sunt censenda.

Thorema 8.

42. Si dum termini progressionis $1, x, x^2, x^3, x^4$, etc. per numerum N ad x primum diuidantur, residua fuerint $1, a, b, c$, etc. in iisdem quoque occurrent tam singulorum omnes potestates, quam producta quaecunque vel binorum, vel ternorum, vel quotlibet in se multiplicatorum.

Demon-

Demonſtratio.

Naſcantur reſidua a, b, c etc. ex poteſtatibus a^α, x^β, x^γ etc. ac numeros etiam maiores quam N in reſiduis admittendo, ex poteſtatibus $x^{2\alpha}$, $x^{3\alpha}$, $x^{4\alpha}$ etc. orientur reſidua a^2, a^3, a^4 etc. quae igitur etiam in ſerie reſiduorum 1, a, b, c etc. continebuntur. Tum vero poteſtates $x^{\alpha+\beta}$, $x^{\alpha+\gamma}$, $x^{\alpha+\beta+\gamma}$ etc. relinquent reſidua ab, ac, abc etc. quae ergo etiam in ſerie reſiduorum inueniri debebunt. Producta igitur, quomodocunque ex reſiduis 1, a, b, c etc. per multiplicationem formata, omnia in eadem ſerie reſiduorum occurrent, ſi quidem ſingula per ablationem diuiſoris N, quoties id fieri poteſt, ad minimam formam reducantur Q. E. D.

Coroll. 1.

43. Haec indoles reſiduorum eo clarius eluceret, ſi eorum loco ipſae illae poteſtates ipſius x, vnde ſunt orta, ſubſtituantur; tum enim manifeſto non ſolum omnes poteſtates harum poteſtatum, ſed etiam earum producta quaecunque, in reſiduis occurrunt.

Coroll. 2.

44. Neque tamen ideo numerus reſiduorum indeterminatus euadit; quemadmodum enim iam vidimus, ex innumeris poteſtatibus paria reſidua prouenire, ita, ſi omnia haec reſidua, ex mutua multiplicatione nata, ad formam minimam reducantur, ad multitudinem modicam reuocabuntur.

Coroll.

Coroll. 3.

45. Ita si minima potestas, quae per N diuisa iterum vnitatem relinquit, fuerit x^ν, ita vt numerus residuorum 1, a, b, c, etc. sit $= \nu$, tum in eodem numero omnia producta, ex multiplicatione numerorum a, b, c, etc. nata, continebuntur, si quidem ab iis diuisor N toties, quoties fieri potest, auferatur.

Scholion.

46. Vnicum exemplum omnibus dubiis, quae forte circa hanc apparentem residuorum multitudinem nasci possunt, soluendis sufficiet. Sit igitur $x = 2$, et pro diuisore sumatur $N = 15$, qui scilicet ad 2 sit primus; iam singulae binarii potestates per 15 diuisae, sequentia relinquent residua

pot. $1; 2; 2^2; 2^3; 2^4; 2^5; 2^6; 2^7; 2^8; 2^9; 2^{10}$; etc.
res. $1; 2; 4; 8; 1; 2; 4; 8; 1; 2; 4;$ etc.

Potestas igitur, quae primum vnitatem reproducit, est 2^4, a qua residua continuo eodem ordine 1, 2, 4, 8 repetuntur, ita vt tantum quaterna residua diuersa occurrant. Hic iam manifestum est, quomodocunque haec residua in se inuicem multiplicentur, nunquam numeros inde produci, qui non in eodem quaternione includantur; postquam scilicet ablatione diuisoris 15 ad formam minimam fuerint reuocata. In hoc quoque exemplo inter residua non omnes partes ad 15 primae occurrunt, sed inde excluduntur istae partes 7, 14, 13, 14, quae pariter ad 15 sunt primae; vnde distributio

supra

ſupra facta inter partes ad diuiſorem primas, quae in reſiduis occurrunt, et quae non occurrunt, illuſtratur, ad quam potiſſimum in ſequentibus probe reſpiciatur.

Thorema 9.

47. In reſiduis ex diuiſione poteſtatum cuiuspiam numeri per diuiſorem ad eum primum relictis, vel omnes partes ad diuiſorem primae occurrunt, vel numerus partium non occurrentium aequalis erit, vel rationem tenebit multiplam ad numerum partium, quae reſidua conſtituunt.

Demonſtratio.

Sit ſeries poteſtatum $1, x, x^2, x^3, x^4, x^5$ etc. et diuiſor N ad x primus, cuius partium ad ipſum primarum numerus ſit $= n$. Sit porro x^ν minima poteſtas, quae per N diuiſa iterum vnitatem relinquit, ita vt numerus omnium diuerſorum reſiduorum ſit $= \nu$, quae cum omnia ſint ad N numeri primi, eorum numerus erit vel $= n$, vel minor; priorique caſu inter reſidua vtique omnes partes ad N primae occurrent. Conſideremus igitur caſum, quo $\nu < n$, ſintque $1, a, b, c, d$, etc. omnia reſidua ex diuiſione poteſtatum

$$1, x, x^2, x^3, x^4 \ldots\ldots x^{\nu-1}$$

per diuiſorem N relicta, quorum numerus cum ſit $= \nu$, non omnes partes ad N primae ibi occurrent. Sit igitur α huiusmodi pars in reſiduis non occurrens, ac demonſtrari poteſt, nullum quoque horum numerorum αa, αb, αc, αd etc. in reſiduis occurrere. Nam ſi

αa esset residuum potestati x^λ respondens, quia a est quoque residuum ex quapiam potestate, puta x^ς, ortum, foret $x^\lambda = AN + \alpha a$, et $x^\varsigma = BN + a$, ideoque $x^\lambda - \alpha x^\varsigma = (A - \alpha B)N$ per N diuisibile. Cum autem x^ς ad N sit numerus primus, et $x^\lambda - \alpha x^\varsigma = (x^{\lambda-\varsigma} - \alpha)$, numerus $x^{\lambda-\varsigma} - \alpha$ esset per N diuisibilis, sicque potestas $x^{\lambda-\varsigma}$ per N diuisa relinqueret residuum α, contra hypothesin. Cum igitur α, αa, αb, αc, etc. quorum numerus est $= \nu$, sint numeri ad N primi, atque diuisione per N ad partes ad N primas reuocari possint, statim atque vna pars α ad N prima in residuis non reperitur, simul quoque ν eiusmodi partes assignari possunt in residuis non occurrentes. Numerus ergo partium non occurrentium, nisi sit nullus, ad minimum est $= \nu$, ac si praeterea fuerit pars ad N prima β in his non residuis non contenta, denuo habebuntur ν partes nouae in residuis non occurrentes; sicque porro. Quare si non omnes partes ad diuisorem N primae in residuis occurrant, numerus partium non occurrentium necessario est vel $= \nu$, vel $= 2\nu$, vel $= 3\nu$, vel alii cuipiam multiplo ipsius ν; hoc est numeri diuersorum residuorum. Q. E. D.

Coroll. 1.

48. Constituto ergo discrimine inter partes ad diuisorem N primas eas quae sunt residua, et eas quae non sunt residua, ex demonstratione patet, productum ex residuo et non residuo in classe non-residuorum semper contineri. Ita si a sit residuum, α non residuum, productum αa certe non erit residuum.

Coroll.

Coroll. 2.

49. Contra autem iam ſupra vidimus productum ex duobus pluribusue reſiduis in claſſe reſiduorum reperiri. Vnde ſequitur ex vno non-reſiduo et quotcunque reſiduis in claſſe non-reſiduorum occurrere debere.

Scholion.

50. Vis huius demonſtrationis iſto nititur fundamento, quod ſi inter reſidua occurrant partes $1, a, b, c, d$, etc. ad diuiſiorem primae, atque α fuerit etiam pars ad diuiſiorem prima in his reſiduis non contenta, tum producta omnia αa, αb, αc, αd, etc. non ſolum in reſiduis non occurrere, quod quidem perfecte eſt demonſtratum, ſed etiam ea eſſe partes ad diuiſorem N primas, omnesque inter ſe diuerſas; ſeu ſi ea per N, actu diuidantur, relinqui reſidua diuerſa. Illud quidem per ſe eſt perſpicuum; cum enim tam α, quam a, b, c, d, etc. ſint numeri ad N primi, etiam eorum producta ad N prima ſint neceſſe eſt. Quod autem producta αa, αb, αc, αc, etc. ſint omnia ad N relata inter ſe diuerſa, intelligitur, quod ſi verbi gratia duo αa et αb per N diuiſa paria darent reſidua, eorum differentia $\alpha b - \alpha a = \alpha(b-a)$ per N eſſet diuiſibilis, ideoque et $b-a$; id quod hypotheſi, quod a et b ſint diuerſae partes ad N primae, repugnat.

Theorema 10.

51. Exponens minimae poteſtatis x^ν, quae per numerum N ad x primum diuiſa vnitatem relinquit,

vel eſt aequalis numero partium ad N primarum, vel huius numeri ſemiſſis, aliaue eius pars aliquota.

Demonſtratio.

Sit n numerus partium ad N primarum, quarum cum ν conſtituant reſidua, erit numerus non-reſiduorum $= n - \nu$. Vidimus autem hunc numerum eſſe vel $= 0$, vel $= \nu$, vel $= 2\nu$, vel alii cuipiam multiplo exponentis ν. Sit ergo $n - \nu = (m-1)\nu$, ita vt m denotet vel vnitatem, vel alium quemuis numerum integrum, atque hinc obtinebimus $n = m\nu$ et $\nu = \frac{n}{m}$: vnde patet exponentem minimae poteſtatis ipſius x, quae per N diuiſa vnitatem relinquit, eſſe vel $= n$, ſi $m = 1$, vel $= \frac{n}{2}$, ſi $m = 2$, vel in genere eſſe partem quampiam aliquotam numeri n, qui exprimit multitudinem partium ad diuiſorem N primarum. Q. E. D.

Coroll. 1.

52. Si x^ν fuerit minima poteſtas, quae per numerum N ad x primum diuiſa vnitatem relinquit, ſequentes poteſtates idem reſiduum relinquentes ſunt $x^{2\nu}$, $x^{3\nu}$, $x^{4\nu}$, $x^{5\nu}$, etc. neque praetera vllae aliae dantur, quae per N diuiſae vnitatem relinquant.

Coroll. 2.

53. Exponens ergo huius poteſtatis minimae ſemper cum numero partium ad diuiſorem N primarum ita connectitur, vt ſit vel illi ipſi, vel cuipiam eius parti aliquotae, aequalis.

Scholion.

Scholion.

54. Quo haec ratio clarius perſpiciatur, iuuabit nonnullos caſus ſimpliciores perpendiſſe. Sit igitur $x=2$, et pro N ſumamus ſucceſſiue numeros impares, vtpote ad $x=2$ primos, atque exhibeamus minimam poteſtatem binarii, quae per quemque numerum imparem diviſa vnitatem relinquat.

Diuiſor N	num. part. ad eum pr. n	min. pot. 2^ν quae per N diuiſ. vnitatem relinquit.
3	2	2^2 ergo $\nu=n$
5	4	2^4 —— $\nu=n$
7	6	2^3 —— $\nu=\frac{1}{2}n$
9	6	2^6 —— $\nu=n$
11	10	2^{10} —— $\nu=n$
13	12	2^{12} —— $\nu=n$
15	8	2^4 —— $\nu=\frac{1}{2}n$
17	16	2^8 —— $\nu=\frac{1}{2}n$
19	18	2^{18} —— $\nu=n$
21	12	2^6 —— $\nu=\frac{1}{2}n$
23	22	2^{11} —— $\nu=\frac{1}{2}n$
25	20	2^{20} —— $\nu=n$
27	18	2^{18} —— $\nu=n$
29	28	2^{28} —— $\nu=n$
31	30	2^5 —— $\nu=\frac{1}{6}n$

Theorema 11.

55. Si fuerit N ad x numerus primus, et n numerus partium ad N primarum, tum poteſtas x^n vnitate minuta ſemper per numerum N erit diuiſibilis.

Demonſtratio.

Sit enim x^ν minima poteſtas, quae per N diuiſa vnitatem relinquit, eritque ν vel aequalis ipſi numero n, vel parti eius cuipiam aliquotae $\frac{n}{m}$. Cum igitur $x^\nu - 1$ per N ſit diuiſibilis, quia forma $x^{\nu m} - 1$ factorem habet $x^\nu - 1$, etiam iſta forma $x^{\nu m} - 1$, ſeu $x^n - 1$, per N erit diuiſibilis. Q. E. D.

Coroll. 1.

56. Si ergo diuiſor N ſit numerus primus p, neque x per p ſit diuiſibilis, tum ſemper numerus $x^{p-1} - 1$ per numerum primum p erit diuiſibilis, vti quidem dudum demonſtraui.

Coroll. 2.

57. Si praeterea p, q, r, etc. ſint numeri primi, x neque vllum eorum implicet, ex hoc theoremate ſequitur,

has formas	fore diuiſibiles per
$x^{p-1} - 1$	p
$x^{p(p-1)} - 1$	pp
$x^{(p-1)(q-1)} - 1$	pq
$x^{pp(p-1)} - 1$	p^3
$x^{p(p-1)(p-1)} - 1$	ppq
$x^{(p-1)(q-1)(r-1)} - 1$	pqr.

Coroll.

Coroll. 3.

58. Si x et y sint primi ad diuisorem N, cuius partium ad eum primarum numerus sit $= n$, quia tam $x^n - 1$, quam $y^n - 1$, est diuisibilis per N, erit etiam $x^n - y^n$ semper diuisibilis per numerum N, quod est Theorema generalius.

Coroll. 4.

59. Proposito ergo numero quocunque N, cuius partium ad ipsum primarum numerus sit $= n$, quicunque numerus ad N primus pro x capiatur, formula $x^n - 1$ semper erit per numerum N diuisibilis.

Coroll. 5.

60. Saepe numero vero etiam euenire potest, vt huiusmodi formula simplicior, veluti $x^{\frac{1}{2}n} - 1$ vel $x^{\frac{1}{3}n} - 1$, vel $x^{\frac{1}{4}n} - 1$ etc. sit per numerum N diuisibilis, quae circumstantia pendet a certa indole numeri x.

Scholion.

61. En ergo nouam demonstrationem Theorematis Fermatiani, quod si fuerit p numerus primus, omnes numeri in hac forma $a^{p-1} - 1$ contenti sint per p diuisibiles, dummodo numerus a non sit per p diuisibilis. Duas autem iam dudum huius theorematis dederam demonstrationes; sed ea quam hic exhibui, iis praestare videtur, quod non solum ad numeros primos

mos adſtringitur. Quicunque enim numerus N pro diviſore accipiatur, dummodo a ad eum ſit primus, hic numerus $a^n - 1$ ſemper per N erit diuiſibilis, ſiquidem n denotet numerum partium ad N primarum, quae propoſitio multo latius patet, quam Fermatiana. Ex quo eo magis vtilitas Theorematum primorum elucet, quibus numerum partium ad quemque numerum primarum definiui, quae ſine hac applicatione nimis ſterilia videri potuiſſent.

SVPLE-