

THEOREMATA ARITHMETICA

NOVA METHODO DEMONSTRATA.

Auctore

L. EULERO.

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, ubi insignes numerorum proprietates erutae reperiuntur ac demonstratae. Quo magis autem deinceps numerorum indolem et affectiones Mathematici sunt scrutati, multo plures eorum proprietates observauerunt, vnde pulcherrima Theoremata numerorum naturam illustrantia derivauerunt, 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* relictâ habetur, quorum demonstrationes maximam partem se inuenisse affirmavit, quas cum eius scriptis interuisse in eximium huius scientiae detrimentum non parum est dolendum. Quot autem talium Theorematum demonstrationes vel sunt cogitatae, vel restitutaе, in iis certe multo maioris ingenii elucet, quam vix in vlllo alio demonstrationum genereprehendimus; unde in hoc negotio non tam utilitas, 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, utilitate 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, affirmavit, cuius Theorematis iam geminam dedi demonstrationem. Nunc autem idem in latiori sensu contemplor, atque in genere, si diuisor non sit numerus primus, sed quicumque N , inuestigo, cuiusmodi exponentem potestati cuiusque tribui oporteat, ut expressio $a^n - 1$ semper sit diuisibilis per numerum N , dummodo numerus a cum eo nullum habeat diuisorem communem. Inueni au-

tem hoc semper usu 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 usum habere, atque ad alias magis absconditas numerorum proprietates aditum parere, videntur. His autem praemissis, demonstratio veritatis propositae ita est comparata, ut maiore attentione non indigna videatur.

Theorema I.

I. Si per numerum quemcunque n termini progressionis arithmeticae cuiuscunque, cuius differentia sit numerus ad n primus, diuidantur, inter residua occurrunt 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 unitatem habeat diuisorem communem, ita ut 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.

Adi

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

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

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 $(\nu - \mu)d$ vtiq; 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:

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

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,
K 3 existente

existente a numero quocunque et ν minore quam n , qui per numerum n fit 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 fit 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 demonstrauius, id de tota progressionem 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:

$$a, a+b \dots a+(n-1)b \mid a+nb \dots a+(2n-1)b \mid a+2nb \dots a+(n-1)b \mid$$

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

duorum cognoscere velimus, sufficit unicam periodum examinasse.

Theorema 2.

6. In progressionē 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:

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

Quoniam igitur, si hi termini per numerum n diuidantur, inter residua occurrunt omnes plane numeri ipso n minores; ponamus ex termino quocunque $a+vd$ resultare residuum r , ac manifestum est, si r fuerit numerus ad n primus, illum quoque terminum $a+vd$ ad n fore primum, sin autem r cum n habeat quempiam diuisorem communem, idem quoque erit diuisor communis numerorum n et $a+vd$. 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 $\equiv n-1$; in illa etiam progressionem arithmetica omnes termini praeter unum 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 progressionem 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 progressionem 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 usum, hic autem ea solum adhibere visum est ad hanc quaestionem enodandam: *Proposito numero quocunque n , quot inter numeros ipso minores futuri sunt ad eundem numerum*

rum *n* primi? Statim quidem patet si *n* sit numerus primus, omnes numeros ipso minores simul ad eum fore primos, eorumque ideo numero 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: unde reliqui 43 omnes cum 60 diuisores habent communes. Moneri hic conuenit, unitatem ad omnes plane numeros esse numerum primum, etiam si omnium sit diuisor; id quod ex definitione est euidens, qua numeri dicuntur esse inter se primi, qui praeter unitatem aliam nullam 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 unitates 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:

$p, 2p, 3p, 4p \dots p^m - p$
 Tom. VIII. Nou. Comm. L quo-

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 $= p p - p = p(p-1)$; reliqui, quorum numerus est $p-1$, ad $n = p^2$ erunt compositi, seu per p divisibiles.

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 divisibiles, 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 Theorematis adhibendis istam quaestionem latius patentem resolvere 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 unitate 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

L 2

quoque

quoque ad q sunt primi. Considerentur ergo series verticales, quarum numerus est $p-1$; quaelibet autem continet q terminos in arithmetica progressionē crescens, differentia existente p , quae est ad q numerus primus. In qualibet ergo serie verticali omnes termini praeter unum ad q erunt primi (per §. 7.); unde 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:

$p, 2p, 3p, 4p, \dots, (q-1)p$
 deinde inter eosdem sunt $p-1$ numeri per q diuisibiles, nempe:

$q, 2q, 3q, 4q, \dots, (p-1)q$
 qui cum ab illis omnes sint diuersi, omnino habentur
($q-1$)

$(q-1) + (p-1) = p+q-2$ numeri, qui ad p q 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 sunt 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 plurimum 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 $1, \alpha, \beta, \gamma, \dots, \omega$ 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 unitate usque ad numerum propositum AB, quos sequens schema exhibebit:

$1,$	$\alpha,$	$\beta,$	\dots	ω
$A+1,$	$A+\alpha,$	$A+\beta$	\dots	$A+\omega$
$2A+1,$	$2A+\alpha,$	$2A+\beta$	\dots	$2A+\omega$
$3A+1,$	$3A+\alpha,$	$3A+\beta$	\dots	$3A+\omega$
\vdots	\vdots	\vdots	\vdots	\vdots
\vdots	\vdots	\vdots	\vdots	\vdots
\vdots	\vdots	\vdots	\vdots	\vdots

$(B-1)A+1, (B-1)A+\alpha, (B-1)A+\beta, \dots (B-1)A+\omega.$

Hic singulae series horizontales continent a terminos, numerusque omnium serierum horizontalium est $=B$; unde 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, ut hoc modo relinquuntur, 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 progressionē 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 hypothēsin $=b$. 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 adiciatur, qui sit ad utrumque 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 resoluū 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:

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

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
p^2	$p(p-1)$	3	2
p^3	$p^2(p-1)$	4	2
p^4	$p^3(p-1)$	5	4
p^5	$p^4(p-1)$	6	2
p^6	$p^5(p-1)$	7	6
p^7	$p^6(p-1)$	8	4
p^8	$p^7(p-1)$	9	6
p^9	$p^8(p-1)$	10	4
p^{10}	$p^9(p-1)$	11	10
p^{11}	$p^{10}(p-1)$	12	4
p^{12}	$p^{11}(p-1)$	13	12
p^{13}	$p^{12}(p-1)$	14	6
p^{14}	$p^{13}(p-1)$	15	8
p^{15}	$p^{14}(p-1)$	16	8
p^{16}	$p^{15}(p-1)$	17	16
p^{17}	$p^{16}(p-1)$	18	6
p^{18}	$p^{17}(p-1)$	19	18
p^{19}	$p^{18}(p-1)$	20	8
p^{20}	$p^{19}(p-1)$	21	12
p^{21}	$p^{20}(p-1)$	22	10
p^{22}	$p^{21}(p-1)$	23	22
p^{23}	$p^{22}(p-1)$	24	8
p^{24}	$p^{23}(p-1)$	25	20

Coroll.

Coroll. 5.

26. Hinc igitur proposito numero quocunque multitudo partium ad eum primarum expedite definitur. Veluti, si proponatur 360, cum sit $360 = 2^3 \cdot 3^2 \cdot 5$, erit multitudo partium ad 360 primarum $= 4 \cdot 6 \cdot 4 = 96$.

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:

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

Tom. VIII. Non. Comm.

M

Demon-

Demonstratio.

Com 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 unitas, propterea quod inter potestates ipsius x etiam referri debet $x^0 = 1$. Vtrum autem praeter unitatem etiam omnes reliquae partes ad N primae inter residua occurrant, nec ne? mox videbimus.

Coroll. 3.

31. Si pro x capiatur unitas, omnia residua erunt unitates, quicumque numerus pro N fuerit assumptus. 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 reperieatur 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, utique fieri potest, ut 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 a, b, c, d, e, \dots quarum numerus sit $=n$, inter residua memorata, vel omnes istae partes occurrant, 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 distribuuntur, quarum altera continebit partes in residuis occurrentes, altera vero partes in residuis non occurrentes.

Theorema 7.

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

Demonstratio.

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

tibus residuis redeat; ac dico: unitatem esse id residuum, quod omnium primum sit rediturum. Quod si quis neget, sit x^u ea potestas, cuius residuum primum in sequentibus ex potestate x^{u+v} redeat; cum igitur potestates x^u et x^{u+v} aequalia praebeant residua, earum differentia $x^{u+v} - x^u = x^u(x^v - 1)$ per numerum N erit diuisibilis. Verum producti $x^u(x^v - 1)$ factor prior ad N est numerus primus, ergo alter $x^v - 1$ per N diuisibilis sit necesse est. Hinc autem potestas x^v per N diuisa residuum daret $= 1$, sicque unitas inter sequentia residua citius redibit, quam residuum potestatis x^u , quippe quod per hypothesin demum in potestate altiore x^{u+v} recurrit. Ex quo evidens, nullum residuum iterum occurrere posse, nisi ante unitas 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 occurreret primum residuum 1 ; quod si oriatur ex potestate x^v , numerus praecedentium residuorum diuersorum erit $= \gamma$.

Coroll. 2.

37. Quando autem potestas x^v residuum dat 1 , idem quod primus terminus x^0 , potestas sequens x^{v+1} idem dabit residuum quod x^1 ; et sequentium quaecunque x^{v+2} idem quod potestas x^2 . Cum enim differ-

rentia

rentia $x^{\nu+\mu} - x^{\mu} = x^{\mu}(x^{\nu} - 1)$ fit diuisibilis per N , necesse est, ut 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 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 $x^{\mu}, x^{\mu+\nu}, x^{\mu+2\nu}, x^{\mu+3\nu}, x^{\mu+4\nu}$ etc. aequalia residua suppeditabunt.

Coroll. 4.

39. Si igitur x^{ν} fuerit infima potestas, quae post $x^{\nu} = 1$ iterum unitatem pro residuo praebeat, numerus diuersorum residuorum erit ν . Cum ergo numerus partium ad numerum N primarum sit $=n$, fieri certe nequit, ut 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. usque ad x^n continetur, inter eas certe una saltem reperietur praeter primum terminum 1 , quae per N diuisa unitatem relinquat. Plures fortasse huiusmodi potestates aliquando, sed pauciores una 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 parvus accipiatur. Ita si in divisione cuiuspiam numeri per N relinquatur $N+a$, hoc residuum aequivalens ipsi a censei debet; hincque, si de residuis sermo sit, omnes hi numeri a , $N+a$, $2N+a$, $3N+a$, etc. instar vnius residui a sunt considerandi. Scilicet: multipla quaecumque diuisoris N siue adiecta, siue demta a quopiam residuo a , eius naturam non mutant, atque hoc modo etiam numeri negatiui commode inter residua referuntur; veluti $a-N$ pro eodem residuo est habendum ac a ; et residuum $-x$ aequualet residuo $N-x$. Ex his conficitur, omnes numeros, qui per N diuisi idem exhibeant residuum a , pro eodem residuo haberi posse, ex quo enim numero per diuisionem quotum nimis paruum sumendo oritur residuum, vel $N+a$, vel $2N+a$, vel $3N+a$ etc. ex eodem, quotum plenum sumendo, nascitur residuum a ; tum vero indidem, si quotus capiatur nimis magnus, obtinebuntur residua negatiua $a-N$, vel $a-2N$, vel $a-3N$ etc. quae ergo etiam ab a non discrepare sunt censenda.

Thorema 8.

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

Demon-

Demonstratio.

Nascantur residua a, b, c etc. ex potestatibus a^x, x^b, x^c etc. ac numeros etiam maiores quam N in residuis admittendo, ex potestatibus x^{2a}, x^{3a}, x^{4a} 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 $x^{a+\beta}, x^{a+\gamma}, x^{a+\beta+\gamma}$ etc. relinquent residua ab, ac, abc etc. quae ergo etiam in serie residuorum inueniri debent. Producta igitur, quomocunque ex residuis $1, a, b, c$ etc. per multiplicationem formata, omnia in eadem serie residuorum occurrunt, 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, substituuntur; 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 unitatem relinquit, fuerit x^n ; ita ut numerus residuorum $1, a, b, c$, etc. sit $\equiv 1$, 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 fit 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 unitatem reprodecit, est 2^4 , a qua residua continuo eodem ordine 1, 2, 4, 8 repetuntur, ita ut tantum quaterna residua diuersa occurrant. Hic iam manifestum est, quomocumque 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; unde 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^v minima potestas, quae per N diuisa iterum unitatem relinquit, ita vt numerus omnium diuersorum residuorum sit $=v$, 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 $v < n$, sintque $1, a, b, c, d$, etc. omnia residua ex diuisione potestatum

$$1, x, x^2, x^3, x^4, \dots, x^{v-1}$$

per diuisorem N relictis, quorum numerus cum sit $=v$, non omnes partes ad N primae ibi occurrent. Sit igitur a huiusmodi pars in residuis non occurrens, ac demonstrari potest, nullum quoque horum numerorum aa, ab, ac, ad etc. in residuis occurrere. Nam si

Tom. VIII. Nou. Comm.

N

aa

aa esset residuum potestati x^λ respondens, quia a est quoque residuum ex quapiam potestate, puta x^μ , ortum, foret $x^\lambda = AN + aa$, et $x^\mu = BN + a$, ideoque $x^\lambda - ax^\mu = (A - aB)N$ per N diuisibile. Cum autem x^μ ad N sit numerus primus, et $x^\lambda - ax^\mu = (x^{\lambda-\mu} - a)$, numerus $x^{\lambda-\mu} - a$ esset per N diuisibilis, sicque potestas $x^{\lambda-\mu}$ per N diuisa relinqueret residuum a , contra hypothesin. Cum igitur a, aa, ab, ac , 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 a 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 cuiuspiam multiplo ipsius ν ; hoc est numeri diuersorum residuorum. Q. E. D.

Coroll. I.

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, a non-residuum, productum aa 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 quocunque 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 diuisorem primae, atque a fuerit etiam pars ad diuisorem prima in his residuis non contenta, tum producta omnia aa, ab, ac, ad , 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 a , quam a, b, c, d , etc. sint numeri ad N primi, etiam eorum producta ad N prima sint necesse est. Quod autem producta aa, ab, ac, ad , etc. sint omnia ad N relata inter se diuersa, intelligitur, quod si verbi gratia duo aa et ab per N diuisa paria darent residua, eorum differentia $ab - aa = a(b - a)$ per N esset diuisibilis, ideoque et $b - a$; id quod hypothese, quod a et b sint diuersae partes ad N primae, repugnat.

Theorema 10.

51. Exponens minimae potestatis x^y , quae per numerum N ad x primum diuisa unitatem relinquit,
 $N - 2$ vel

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 constituent residua, erit numerus non-residuorum $= n - \nu$. Vidimus autem hunc numerum esse vel $= 0$, vel $= \nu$, vel $= 2\nu$, vel alii cuiuspiam multiplo exponentis ν . Sit ergo $n - \nu = (m - 1)\nu$, ita ut m denotet vel unitatem, vel alium quemvis numerum integrum, atque hinc obtinebimus $n = m\nu$ et $\nu = \frac{n}{m}$: unde patet exponentem minimae potestatis ipsius x , quae per N diuisa unitatem 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 unitatem 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 unitatem relinquant.

Coroll. 2.

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

Scholion.

Scholion.

54. Quo haec ratio clarius perspiciatur, iuvabit 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 diuisa unitatem relinquat.

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

N 3

Theore-

Theorema II.

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

Demonstratio.

Sit enim x^y minima potestas, quae per N diuisa unitatem relinquit, eritque y vel aequalis ipsi numero n , vel parti eius cuiusdam aliquotae $\frac{n}{m}$. Cum igitur $x^y - 1$ per N sit diuisibilis, quia forma $x^{ym} - 1$ factorem habet $x^y - 1$, etiam ista forma $x^{ym} - 1$, 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, uti quidem dudum demonstraui.

Coroll. 2.

57. Si praeterea p, q, r , etc. sint numeri primi, x neque ullum 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, ut huiusmodi formula simplicior, veluti $x^{\frac{1}{2}n} - 1$ vel $x^{\frac{2}{3}n} - 1$, vel $x^{\frac{1}{3}n} - 1$ 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 desideram demonstrationes; sed ea quam hic exhibui, iis praestare videtur, quod non solum ad numeros primos

104 THEOREMAT. ARITHMET. NOVA etc.

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

SUPLE.