1774

Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia

Leonhard Euler

DEMONSTRATIONES CIRCA RESIDVA EX DIVISIONE POTESTATVM PER NVMEROS PRIMOS RESVLTANTIA.

Auctore

L. EVLERO.

Hypothesis.

1.

Si termini progressionis geometricae ab vnitate incipientis per numerum primum P diuidantur, residua inde nata litteris 1, α, β, γ, δ etc. denotabo, hoc modo:

Progr. Geom.	$1, a, a^2, a^3, a^4, a^5, a^6$ etc.
Residua	$1, \alpha, \beta, \gamma, \delta, \varepsilon, \zeta$ etc.

Conclusiones.

2. Omnia haec residua sunt minora diuisore P; quamdiu enim termini progressionis geometricae diuisore P sunt minores, residua ipsis sunt aequalia; cum autem diuisorem P superant, auferendo ab iis diuisorem P, quoties fieri potest, residua tandem ipso P minora relinqui necesse est.

3. Si numerus a sit primus ad diuisorem P, hoc est si neque ipsi sit aequalis, neque eius mul-

tiplo cuipiam, nulla quoque eius potestas per P erit diuisibilis; neque ergo in residuis cyphra vnquam occurret.

4. Cum omnia residua sint diuisore P minora, multitudo autem numerorum diuisore P minorum sit $= P - 1$, plura residua diuersa occurrere nequeunt quam $P - 1$. Quare cum series residuorum sit infinita, eadem residua in ea saepius recurrere debent.

5. Ex quolibet residuo veluti ε sequens ζ facile definitur. Cum enim sit $\varepsilon = a^5 - mP$ et $\zeta = a^6 - nP$, erit $\zeta - a\varepsilon = (ma - n)P$, hincque $\zeta = a\varepsilon - (n - ma)P$. Quare a producto $a\varepsilon$ auferatur diuisor P quoties fieri potest, ac relinquetur residuum sequens ζ.

6. Respectu numeri primi P omnes numeri in certos ordines distribui possunt, ad eundem ordinem referendo omnes eos numeros, qui per P diuisi idem relinquunt residuum, hi ergo ordines erunt:

I.	0,	P	2P,	3P,	4P	mP
II.	1,	P+1,	2P+1,	3P+1,	4P+1	$mP+1$
III.	2,	P+2,	2P+2,	3P+2,	4P+2	$mP+2$
IV.	3,	P+3,	2P+3,	3P+3,	4P+3	$mP+3$

etc.

7. Pro quolibet ergo numero primo P tot habentur numerorum ordines, quot vnitates in numero P continentur; et quilibet ordo determinatur residuo, quod omnibus numeris eius ordinis est commune; hocque residuum in quouis ordine locum occupat primum.

8. Cum

8. Cum cuiusque ordinis natura residuo ipsi proprio determinetur, quilibet cuiusque ordinis numerus eius naturam perinde declarat, ac primus, qui ipsum residuum exhibet. Hinc nihil impedit, quominus idem residuum ε per quemlibet alium numerum eiusdem ordinis $m\,P + \varepsilon$ denotetur.

9. Ita idem residuum ε non solum per numeros positiuos $\varepsilon + P$, $\varepsilon + 2\,P$ etc. indicare licebit, sed etiam per negatiuos $\varepsilon - P$, $\varepsilon - 2\,P$ etc. Cum igitur, si ε sit diuisoris P semisse maius, $\varepsilon - P$ eodem sit minus, patet numeros negatiuos admittendo, omnia residua numeris, qui diuisoris P semissem non superent, exprimi posse.

Obseruationes.

10. Proposito diuisore primo P, prout progressionis geometricae radix a constituatur, fieri potest, vt in residuis vel omnes numeri ipso P minores occurrant, vel non omnes. Si enim sumatur radix $a = 1$, omnia residua in vnitatem abeunt, ac si sumatur $a = P - 1$, series residuorum prodit:

$$1,\ P-1,\quad 1,\ P-1,\quad 1,\ P-1 \text{ etc.}$$
$$\text{vel } +1,\ -1,\ +1,\ -1,\ +1,\ -1 \text{ etc. } (9).$$

11. Quod autem interdum omnes numeri diuisore P minores in residuis occurrunt, vnico exemplo declarasse sufficiat; sit scilicet $P = 7$ et sumatur radix $a = 3$, habebitur:

progr. geom.	$1, 3, 3^2, 3^3, 3^4, 3^5, 3^6, 3^7, 3^8, 3^9$ etc.
Residua	$1, 3, 2, 6, 4, 5, 1, 3, 2, 6$ etc.

12. Si

12. Si pro eodem diuiſore $P = 7$ radici a alii valores tribuantur, ſeries reſiduorum ſe habebunt vt ſequitur:

$\begin{cases} \text{Progr. geom.} & 1,\ 2,\ 2^2,\ 2^3,\ 2^4,\ 2^5,\ 2^6,\ 2^7,\ 2^8,\ 2^9 \text{ etc.} \\ \text{Reſidua} & 1,\ 2,\ 4,\ 1,\ 2,\ 4,\ 1,\ 2,\ 4,\ 1 \text{ etc.} \end{cases}$

$\begin{cases} \text{Progr. geom.} & 1,\ 4,\ 4^2,\ 4^3,\ 4^4,\ 4^5,\ 4^6,\ 4^7,\ 4^8,\ 4^9 \text{ etc.} \\ \text{Reſidua} & 1,\ 4,\ 2,\ 1,\ 4,\ 2,\ 1,\ 4,\ 2,\ 1 \text{ etc.} \end{cases}$

$\begin{cases} \text{Progr. geom.} & 1,\ 5,\ 5^2,\ 5^3,\ 5^4,\ 5^5,\ 5^6,\ 5^7,\ 5^8,\ 5^9 \text{ etc.} \\ \text{Reſidua} & 1,\ 5,\ 4,\ 6,\ 2,\ 3,\ 1,\ 5,\ 4,\ 6 \text{ etc.} \end{cases}$

13. Vt omnes variationes, quae in ſerie reſiduorum locum habere poſſunt, obtineantur, ſufficit radici a omnes valores diuiſore P minores tribuiſſe; ſi enim loco a ſumatur $a + P$, ex progreſſione geometrica $1,\ a + P,\ (a + P)^2,\ (a + P)^3$ etc. eadem reſiduorum ſeries recurrit, quae ex progreſſione geometrica $1,\ a,\ a^2,\ a^3,\ a^4$ etc.

14. Quemadmodum in reſiduis etiam numeros negatiuos admittimus (9) vt ea infra ſemiſſem diuiſoris P deprimamus, ita etiam pro radice progreſſionis geometricae a numeros negatiuos aſſumere licet, ac tum habebitur:

Progr. geom. $1, -a, +a^2, -a^3, +a^4, -a^5, +a^6, -a^7$ etc.
reſidua $1, -\alpha, \ \beta, -\gamma, \ \delta, -\varepsilon, \ \zeta, -\eta$ etc.

15. Sumta autem radice $-a$, eadem reſidua oriuntur, ac ſi radix poneretur $P - a$; vnde patet pro caſibus, quibus radix a ſemiſſem diuiſoris P ſuperat, reſidua ex caſibus quibus eſt $a < \frac{1}{2} P$ facile colligi.

16.

16. Quodsi loco radicis a successiue omnes numeri diuisore P minores substituantur, series residuorum inde natae vel erunt completae vel incompletae: *completas* scilicet appello, in quibus omnes numeri diuisore P minores occurrunt, *incompletas* vero, vbi quidam horum numerorum ex serie residuorum excluduntur.

17. Quoniam vidimus pro quouis diuisore P dari eiusmodi valores radicis a, veluti si $a = 1$ et $a = P - 1$, ex quibus series residuorum incompletae resultant; hinc nascitur quaestio; *an semper eiusmodi progressiones geometricae exhiberi queant, vnde series residuorum completae oriantur.*

18. Huiusmodi radices progressionis geometricae, quae series residuorum completas producunt, *primitiuas* appellabo. Ita supra vidimus pro diuisore $P = 7$ radices *primitiuas* esse 3 et 5. Num autem pro omnibus diuisoribus primis dentur radices primitiuae, quaestio est altioris indaginis, infra decidenda.

Lemmata.

19. Cum in serie residuorum termini praecedentes tandem recurrere debeant, *primus qui recurrit semper est vnitas. Demonstratio.* Ponamus enim aliud quoduis residuum ε ex potestate a^{μ} natum recurrere, antequam vnitas recurrat, idque secunda vice ex potestate $a^{\mu+\nu}$ prodire. Cum igitur sit $\varepsilon = a^{\mu} - m\,P$ et $\varepsilon = a^{\mu+\nu} - n\,P$, erit $a^{\mu+\nu} - a^{\mu} = (n - m)\,P$ ideoque $a^{\mu}\,(a^{\nu} - 1)$ multiplum ipsius P; at quia a^{μ} per

 nume-

numerum primum P diuidi nequit, (radix enim a diuisore P minor ideoque ad eum prima statuitur), necessario alter factor $a^{\nu} - 1$ per P diuisionem admittet, hincque potestas a^{ν} per P diuisa vnitatem relinquet; quae potestas cum inferior sit quam $a^{\mu+\nu}$ euidens est, residuum ε ante recurrere non posse, quam vnitas recurrerit.

20 Statim atque in serie residuorum $1, \alpha, \beta, \gamma, \delta$ etc. vnitas iterum occurrit, deinceps eadem residua eodem ordine vti ab initio iterum recurrent.

Dem. Oriatur enim vnitas secunda vice ex potestate a^{ν} ac sequens residuum erit a, 1 (5) $= a$, idem quod ex secundo termino a nascebatur, ideoque α, post quod denuo sequentur residua β, γ, δ etc. eodem ordine vti ab initio.

21. Si a sit radix primitiua, eius potestas a^{P-1} per diuisorem primum P diuisa vnitatem relinquet.

Dem. Quia a est radix primitiua in serie residuorum omnes numeri diuisore P minores occurrunt, quorum multitudo est $P-1$; ex totidem ergo progressionis geometricae terminis $1, a^1, a^2, a^3$ etc. orientur necesse est; sequorum vltimus erit a^{P-2} sequens ergo terminus a^{P-1} aliquod ex residuis praecedentibus reproducet, quod autem necessario est vnitas (19).

22. Si progressio geometrica $1, a, a^2, a^3, a^4$ etc. seriem residuorum *incompletam* producat; numerus residuorum diuersorum erit pars aliquota numeri $P-1$ hoc est diuisoris primi P vnitate minuti.

Dem.

Dem. Sit numerus residuorum diuersorum $1, \alpha, \beta, \gamma, \delta$ etc. ex hac progressione geometrica natorum $= r$, qui ergo per hypothesin minor est quam $P - 1$, ita vt quidam numeri, qui sint $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ etc. eorumque multitudo $= P - 1 - r$, ex serie residuorum excludantur. Iam dico, quia $\mathfrak{A}$ in serie residuorum non reperitur, ibidem quoque nec $\alpha\mathfrak{A}$, nec $\beta\mathfrak{A}$, nec $\gamma\mathfrak{A}$ etc. occurrere posse. Si enim $\varepsilon\mathfrak{A}$ esset residuum, quia ε ex certa potestate radicis a, quae sit a^ν, nascitur, loco $\varepsilon\mathfrak{A}$ spectare licet $a^\nu\mathfrak{A}$, vnde sequentia residua forent $a^{\nu+1}\mathfrak{A}$, $a^{\nu+2}\mathfrak{A}$, $a^{\nu+3}\mathfrak{A}$ etc. et in genere $a^n\mathfrak{A}$, quia autem datur potestas a^n vnitatem relinquens, hoc residuum foret $\mathfrak{A}$ contra hypothesin. Hinc dato vno non-residuo $\mathfrak{A}$, simul dantur r non-residua; quae si nondum multitudinem numerorum $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ etc. quorum numerus est $P - 1 - r$ exhauriant, de nouo r non-residua accedunt, sicque porro; vnde numerus $P - 1 - r$ necessario erit multiplus ipsius r, sit ergo $P - 1 - r = nr$, fiet $r = \frac{P-1}{n+1}$, ac propterea numerus residuorum r semper est pars aliquota numeri $P - 1$.

23. Quicunque valor diuisore primo P minor radici a tribuatur, potestas a^{P-1} per P diuisa vnitatem relinquit, seu formula $a^{P-1} - 1$ per P erit diuisibilis.

Dem. Sit r numerus omnium residuorum diuersorum $1, \alpha, \beta, \gamma, \delta$ etc. quae ergo nascuntur ex progressione geometrica

$$1, a, a^2, a^3, a^4 \ldots\ldots\ldots a^{r-1}$$

ſequens igitur poteſtas a^r vnitatem pro reſiduo habebit, eritque forma $a^r - 1$ per diuiſorem P diuiſibilis. Quia vero r eſt pars aliquota numeri $P - 1$, illa forma $a^{P-1} - 1$ per hanc $a^r - 1$ erit diuiſibilis, ideoque etiam per ipſum diuiſorem P.

24. In ſerie reſiduorum $1, \alpha, \beta, \gamma, \delta$ etc. ſiue fuerit completa ſiue incompleta, ſimul producta ex binis, ternis quaternis etc. hincque etiam ſingulorum poteſtates quaecunque, ſiquidem per diuiſorem P deprimantur, occurrunt.

Dem. Si enim poteſtas a^m reſiduum relinquat μ, et poteſtas a^n reſiduum ν, erit $a^m = ..P + \mu$ et $a^n = ..P + \nu$ vbi duo puncta .. loco cuiusuis indicis integri ſcribo; hincque $a^{m+n} = ..P + \mu\nu$, ita vt poteſtas a^{m+n} reſiduum $\mu\nu$ ſit relictura. Quare cum productum binorum quorumcunque reſiduorum in ſerie reſiduorum occurrat, propoſitum eſt manifeſtum.

25. Datis duobus reſiduis μ et ν in ſerie reſiduorum etiam aliquod reperietur ω vt ſit $\nu = \mu\omega$ vel $\nu = \mu\omega - ..P$.

Dem. Oriantur enim reſidua μ et ν a poteſtatibus a^m et a^n ac ſit ω reſiduum a poteſtate a^{n-m} vel hac $a^{P-1+n-m}$ ſi forte fuerit $n < m$, eritque poteſtatis $a^n = a^m . a^{n-m}$ reſiduum $= \mu\omega - ..P$ ideoque $\nu = \mu\omega - ..P$.

26. Cum vnitas ſemper in ſerie reſiduorum contineatur, cuique reſiduo μ reſpondebit ibidem aliud

aliud quoddam ω vt fit $\mu\omega = 1$ feu $\mu\omega = 1 + .. P$. Huiusmodi bina refidua *focia* appellabo. Vnde patet, in omni ferie refiduorum terminos ita fociatim exhiberi poffe, vt bina quaeque fibi fint focia. Hoc tantum notetur, vnitatem fibi ipfi effe *fociam*, ac fi -1 occurrat, focium quoque ipfi effe aequalem.

27. His praemiffis, quae alibi fufius pertractavi, ad fequentia Theoremata progredior; in quibus plures nouae veritates ex principiis prorfus fingularibus demonftrabuntur, ad quas per methodos adhuc vfurpatas acceffus nimis difficilis videtur.

Theorema.

28. Vt forma $x^n - 1$ per numerum primum P diuifibilis euadat, fumendo $x < P$, id pluribus quam n modis fieri nequit.

Demonftratio.

A cafibus fimpliciffimis inchoemus, ac primo ftatim manifeftum eft formam $x^1 - 1$ per numerum primum P vnico modo diuifibilem effe poffe fumendo $x = 1$, cum valores ipfius x diuifore P maiores excludantur.

Vt forma $x^2 - 1$ diuifionem per numerum primum P admittat vel $x - 1$ vel $x + 1$ diuifionem admittere debet; priori cafu fit $x = 1$ pofteriori $x = P - 1$: neque vllo alio modo id euenire poteft, fiquidem cafus $x > P$ excluduntur. Forma $x^3 - 1 = (x - 1)(xx + x + 1)$ per P diuifibilis eft

 primo

primo ſi $x = 1$, tum vero ſi $xx + x + 1 = m$P. quod ſi eueniat caſu $x = a$, etiam caſu $x = a^2$ ſuccedet, altiores enim poteſtates ob $a^3 - 1$ diuiſ. per P ideoque reſiduum ipſius $a^3 - 1$ ad praecedentes reducuntur. Iam vero dico praeter hos tres caſus alios dari nullos; ſi enim diuiſio ſuccederet quoque caſu $x = b$, ob $aa + a + 1$ et $bb + b + 1$ per P diuiſibiles differentia $(a - b)(a + b + 1)$ etiam eſſet diuiſibilis hoc eſt vel $a - b$ vel $a + b + 1$, prius daret $b = a$, poſterius ab $aa + a + 1$ ablatum praeberet $aa - b = m$P hoc eſt $b = aa$, qui ſunt caſus iam enumerati. Vnde pluribus quam tribus modis diuiſio non ſuccedit.

Iam pro forma $x^n - 1$ in genere obſeruo, ſi ea per numerum primum P fuerit diuiſibilis caſu $x = a$; vt ſit $x - a$ diuiſor formae $x^n - 1 - m$P, tum facta diuiſione oriri formam vno gradu inferiorem per P diuiſibilem reddendam; quod ſi praeſtet valor $x = b$ denuo ad formam inferiorem peruenietur, ex quo perinde atque in reſolutione aequationum concluditur, pluribus quam n modis quaeſitum obtineri non poſſe; qui ſi $x = a$ fuerit vnus valor idoneus, erunt

$$x = 1,\ x = a,\ x = a^2,\ x = a^3,\ x = a^4 \ldots x = a^{n-1}$$

quandoquidem a^n iterum vnitati aequiualet.

Scholion.

29. Theorema hoc ita accipi debet, vt forma $x^n - 1$ certe non pluribus quam n modis per numerum primum P diuiſibilis reddi queat, aliis pro x valo-

valoribus non admittendis, nisi qui ipso P sint minores. Cum enim si quispiam valor $x = a$ id praestet, omnes in hac formula $x = a + m P$ idem sint praestaturi, hos omnes pro vnico casu haberi conuenit. Hac lege constituta saepius euenire potest, vt numerus casuum sit minor quam exponens n; veluti si quaestio sit, quot casibus forma $x^5 - 1$ per 7 diuisibilis existat, hoc non 5 sed vnico modo $x = 1$ fieri posse deprehenditur, dum reliqui 4 casus quasi fiunt imaginarii. Ex sequentibus autem patebit, semper quasdam solutiones fieri impossibiles, quoties exponens n non fuerit pars aliquota ipsius $P - 1$. dum contra, quoties n est pars aliquota ipsius $P - 1$ omnes solutiones sunt reales. Ac si $n = P - 1$ tum manifesto totidem habentur solutiones, quia omnes numeri ipso P minores, quorum multitudo est $P - 1$, loco x positi formulam $x^n - 1$ per numerum primum P diuisibilem reddunt (22). Quando autem exponens n maior est quam $P - 1$, veluti $n = P - 1 + k$, tum forma $x^{P-1+k} - 1$, reducitur ad $x^k - 1$, quoniam potestas x^{P-1} ratione residuorum vnitati aequiualere est censenda.

Definitio.

30. Casus proprii, quibus formula $x^n - 1$ per quempiam numerum primum diuisibilis esse potest, sunt ii, qui ipsi cum nulla forma inferiori, vbi exponens n est minor, sunt communes.

Coroll.

Coroll. 1.

31. Quia casus $x = 1$ formulae $x^n - 1$ cum omnibus inferioribus est communis, hunc semper a casibus formulae isti propriis excludi oportet; vnde cum numerus omnium casuum sit n, numerus casuum propriorum saltem vnitate est minor.

Coroll. 2.

32. Si exponens n fuerit numerus primus, formula $x^n - 1$ per nullam inferiorem eiusdem formae diuisibilis est praeter $x^1 - 1$, vnde numerus casuum propriorum est $n - 1$.

Coroll. 3.

33. Sin autem exponens n fuerit numerus compositus puta $n = \mu\nu$, tum formula $x^n - 1$ iisdem casibus est diuisibilis, quibus formulae $x^\mu - 1$ et $x^\nu - 1$, quandoquidem ipsa per has diuisibilis existit; vnde casus harum formularum a casibus propriis formulae $x^n - 1$ sunt segregandi.

Problema.

34. Pro omnibus exponentibus n numerum casuum propriorum definire, quibus formula $x^n - 1$ per quempiam numerum primum P diuisibilis reddi potest, alios pro x valores non admittendo, nisi qui diuisore sint minores.

Solutio.

Solutio.

A numero omnium casuum, qui est $= n$ excludantur casus, quibus formulae inferiores in proposita contentae simul fiunt diuisibiles; aliae autem formulae inferiores veluti $x^{\nu} - 1$ in proposita $x^n - 1$ non continentur, nisi quarum exponens ν est pars aliquota exponentis n. Verum si plures huiusmodi formulae inferiores dentur, ne iidem casus bis vel pluries excludantur, tantum casus cuique proprii excludi debent, quo facto remanebunt casus formulae propositae $x^n - 1$ proprii; hoc modo ab exponentibus minoribus ad continuo maiores facile progredi licet:

formula	numerus casuum propriorum
$x^1 - 1$	1
$x^2 - 1$	$2 - 1 = 1$
$x^3 - 1$	$3 - 1 = 2$
$x^4 - 1$	$4 - 1 - 1 = 2$
$x^5 - 1$	$5 - 1 = 4$
$x^6 - 1$	$6 - 2 - 1 - 1 = 2$
$x^7 - 1$	$7 - 1 = 6$
$x^8 - 1$	$8 - 2 - 1 - 1 = 4$
$x^9 - 1$	$9 - 2 - 1 = 6$
	etc.

Hinc in genere si α, β, γ, δ etc. sint numeri primi, res ita se habebit:

formula	numerus caſuum propriorum
$x^{1}-1$	1
$x^{\alpha}-1$	$\alpha-1$
$x^{\beta}-1$	$\beta-1$
$x^{\gamma}-1$	$\gamma-1$
$x^{\alpha\alpha}-1$	$\alpha\alpha-\alpha=\alpha(\alpha-1)$
$x^{\alpha\beta}-1$	$\alpha\beta-\alpha-\beta+1=(\alpha-1)(\beta-1)$
$x^{\beta\beta}-1$	$\beta\beta-\beta=\beta(\beta-1)$
$x^{\alpha\gamma}-1$	$\alpha\gamma-\alpha-\gamma+1=(\alpha-1)(\gamma-1)$
$x^{\beta\gamma}-1$	$\beta\gamma-\beta-\gamma+1=(\beta-1)(\gamma-1)$
$x^{\gamma\gamma}-1$	$\gamma\gamma-\gamma=\gamma(\gamma-1)$
$x^{\alpha\alpha\alpha}-1$	$\alpha^{3}-\alpha\alpha+\alpha-\alpha+1-1=\alpha\alpha(\alpha-1)$
$x^{\alpha\alpha\beta}-1$	$\alpha\alpha\beta-\alpha\alpha+\alpha-(\beta-1)(\beta-1)-\alpha-\beta+1=\alpha(\alpha-1)(\beta-1)$

vnde colligimus, ſi fuerit $n=\alpha^{\lambda}\beta^{\mu}\gamma^{\nu}$, pro formula $x^{n}-1$ fore numerum caſuum propriorum

$$\alpha^{\lambda-1}(\alpha-1)\beta^{\mu-1}(\beta-1)\gamma^{\nu-1}(\gamma-1).$$

Quae ſi attentius contemplemur, mox deprehendemus pro qualibet formula $x^{n}-1$ tot dari caſus proprios, quot infra exponentem n dantur numeri ad ipſum primi.

Coroll. I.

35. Diuiſore primo exiſtente $=P$, ſi exponens n ſumatur $=P-1$, quia formula $x^{P-1}-1$ certo habet $P-1$ caſus eosque omnes reales, cum x omnes valores ipſo P minores recipere queat; ſi inde expungantur ii, qui huic formulae cum ſimplicioribus ſunt communes, caſus proprii, qui relinquuntur, omnes certo erunt reales.

Coroll.

Coroll. 2.

36. Hinc ſemper eiusmodi dantur numeri diuiſore P minores, qui caſus formulae $x^{p-1} - 1$ proprios exhibent, ita, vt iidem caſus nulli formulae inferiori conueniant.

Scholion.

37. Quamuis haec nimis abſtracta et omni vſu deſtituta videantur; tamen equidem iis ſuperſedere non potui in ſequentibus demonſtrationibus adornandis, vbi imprimis ante omnia eſt oſtendendum, quicunque numerus primus pro diuiſore P accipiatur, ſemper eiusmodi progreſſiones geometricas $1, a, a^2, a^3, a^4$ etc. exhiberi poſſe, vnde ſeries reſiduorum completae reſultent, in quibus ſcilicet omnes numeri diuiſore P minores occurrant, antequam idem reſiduorum ordo reuertatur. Pleriſque forte haec res ita manifeſta videbitur, vt demonſtratione non egeat, cum pro minoribus diuiſoribus primis huiusmodi progreſſiones geometricae ſeries reſiduorum completas praebentes, actu exhiberi queant, pro maioribus autem ratio dubitandi continuo decreſcere videatur. Verum quoniam hoc ſecus euenit pro diuiſoribus non-primis, haec numerorum primorum proprietas vtique demonſtrationem poſtulare eſt viſa.

Theorema.

38. Quicunque numerus primus pro diuiſore P accipiatur; ſemper eiusmodi progreſſio geometrica

1, a, a^2, a^3, a^4 etc. exhiberi poteſt, ex qua ſeries reſiduorum completa oriatur.

Demonſtratio.

Cum poſita in genere progreſſionis geometricae radice x, minore ſemper quam diuiſor P, terminus x^{P-1} per P diuiſus vnitatem relinquat, indeque reſidua eodem ordine vti ab initio reuertantur; oſtendi oportet pro x eiusmodi numerum a aſſumi poſſe, vt a^{P-1} ſit eius infima poteſtas, quae per P diuiſa vnitatem relinquat; quia enim tum in ſerie reſiduorum vnitas ante hunc terminum non occurrit, omnia antecedentia reſidua inter ſe diuerſa ſint neceſſe eſt, quorum numerus cum ſit $= P-1$, omnes numeri diuiſore P minores in ſerie reſiduorum reperientur, eaque propterea erit completa. Res itaque huc redit, vt oſtendatur, non omnes numeros diuiſore P minores ita eſſe comparatos, vt eorum inferior quaepiam poteſtas per P diuiſa vnitatem relinquat. Verum ſi hoc eueniat in poteſtate x^n exiſtente $n < P-1$; iam oſtendimus (§. 21.), eius exponentem n eſſe neceſſario partem aliquotam ipſius $P-1$; cum iam §. 34. docuerim, formam $x^{P-1}-1$ ſemper habere caſus ſibi proprios puta $x=a$, vt nulla inferior diuiſionem per P admittat; perſpicuum eſt poteſtatem a^{P-1} fore infimam, quae per P diuiſa vnitatem relinquat; vnde ſumto tali numero a pro radice progreſſionis geometricae, ex ea ſeries reſiduorum completa oriatur neceſſe eſt.

Scho-

Scholion.

39. Quo haec clarius intelligantur, conueniet pro simplicioribus diuiſoribus primis tales ſeries reſiduorum completas conſpectui exponi, vbi quidem progreſſiones geometricas, vnde naſcuntur, non opus eſt exponi, quia radix ſemper ſecundo termino ſeriei reſiduorum eſt aequalis; ſed ſufficiet generalem progreſſionem in capite poſuiſſe, vt inde exponentes, quibus ſinguli termini in ſeriebus reſiduorum reſpondent, perſpiciantur:

<table>
<tr><th>Diuiſor primus</th><th>$a^0, a^1, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}, a^{12}, a^{13}, a^{14}, a^{15}, a^{16}, a^{17}, a^{18}, a^{19}, a^{20}$ etc.</th></tr>
<tr><td>3</td><td>1, 2 | 1, 2 | 1, 2 | 1, 2 | 1, 2 | 1, 2 | 1, 2 | 1, 2 | 1, 2 | 1, 2 | 1, etc.</td></tr>
<tr><td>5</td><td>1, 2, 4, 3 | 1, 2, 4, 3 | 1, 2, 4, 3 | 1, 2, 4, 3 | 1, 2, 4, 3 | 1, 2 etc.</td></tr>
<tr><td>7</td><td>1, 3, 2, 6, 4, 5 | 1, 3, 2, 6, 4, 5 | 1, 3, 2, 6, 4, 5 | 1, 3, 2, 6 etc.</td></tr>
<tr><td>11</td><td>1, 2, 4, 8, 5, 10, 9, 7, 3, 6 | 1, 2, 4, 8, 5 10, 9, 7, 3, 6 | 1, 2 etc.</td></tr>
<tr><td>13</td><td>1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7 | 1, 2, 4, 8, 3, 6, 12, 11, 9, 5, etc.</td></tr>
<tr><td>17</td><td>1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12 2, 6 | 1, 3, 9, 10, 13, 5 etc.</td></tr>
<tr><td>19</td><td>1, 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10 | 1, 2, 4, 8 etc.</td></tr>
<tr><td>23</td><td>1, 5, 2, 10, 4, 20, 8, 17, 16, 11, 9, 22, 18, 21, 13, 19, 3, 15, 6, 7, 12, 14 | etc.</td></tr>
</table>

Radices igitur, quibus hic pro iſtis diuiſoribus primis ſumus vſi, ſunt primitiuae, quia earum poteſtates omnia diuerſa reſidua diuiſore minora ſuppeditant, quibus exhauſtis demum vnitas recurrit, et ſeries eodem ordine vti ab initio progrediuntur. Via quidem adhuc non patet, tales radices primitiuas pro quouis diuiſore primo inueniendi, neque etiam demonſtratio, qua tales radices primitiuas ſemper dari euici, methodum eas inueniendi declarat.

Pro quouis autem diuisore primo radix huiusmodi primitiua tentando non difficulter elicitur. Veluti pro diuisore 23, primum radicem $a = 2$ assumo, vnde haec series residuorum nascitur:

$$1,\ 2,\ 4,\ 8,\ 16,\ 9,\ 18,\ 13,\ 3,\ 6,\ 12,\ 1$$

quae cum sit incompleta, iam inde patet radicem primitiuam inter numeros exclusos quaeri debere, quorum minimus qui 5 negotium conficere deprehenditur; nisi hoc accidisset; denuo inter numeros exclusos radicem primitiuam quaesiuissem.

Theorema.

40. Si diuisor primus sit $P = 2n + 1$, et a radix primitiua; tum progressionis geometricae $1, a, a^2, a^3$ etc. terminus a^n residuum praebet $2n$ seu -1.

Demonstratio.

Cum a sit radix primitiua, eius potestas a^{2n} per diuisorem $2n+1$ diuisa vnitatem relinquit, neque vlla datur potestas inferior idem praestans; formula ergo $a^{2n} - 1$ per eundem diuisorem erit diuisibilis, neque vlla alia inferior. Cum igitur sit $a^{2n} - 1 = (a^n - 1)(a^n + 1)$, et factor $a^n - 1$ non sit per diuisorem $2n + 1$ diuisibilis, alterum factorem $a^n + 1$ diuisibilem esse necesse est, seu erit $a^n + 1 = m(2n + 1)$ hincque $a^n = m(2n + 1) - 1$ vel $a^n = (m - 1)(2n + 1) + 2n$; vnde manifestum est potestatem a^n per diuisorem $2n + 1$ diuisam relinquere -1 seu $2n$.

Coroll. 1.

41. Si ergo residua ex initio progressionis geometricae 1, a, a^2, a^3 etc. nata sint 1, α, β, γ etc. residua ex terminis a^n, a^{n+1}, a^{n+2}, a^{n+3} etc. nata erunt $-1, -\alpha, -\beta, -\gamma$ etc. seu $2n$, $2n+1-\alpha$, $2n+1-\beta$, $2n+1-\gamma$ etc. cum sit $\alpha = a$, $\beta = a\alpha$, $\gamma = a\beta$ etc. semperque sequens terminus oriatur ex praecedente per radicem a multiplicato.

Coroll. 2.

42. Series ergo residuorum completa, cuius terminorum numerus est $= 2n$, antequam iidem termini recurrant, in duas partes dispescitur $1, \alpha, \beta, \gamma, \delta$ etc. et $-1, -\alpha, -\beta, -\gamma, -$ etc. cuius posterioris termini sunt complementa terminorum prioris; seu residua ex terminis a^λ et $a^{n+\lambda}$ nata simul sumta sunt $= 0$ siue diuisorem $2n+1$ praebent.

Scholion.

43. Quae de binis residuis sociis super sunt obseruata, quorum productum vnitate superat multiplum diuisoris, ea hic ita sunt disposita, vt a medio, quod est -1 vel $2n$ aequidistent. Si enim r et s sint residua ex potestatibus $a^{n+\nu}$ et $a^{n-\nu}$ nata; productum rs erit residuum ex potestate a^{2n} natum, quod cum sit vnitas, erit $rs = 1$ vel $1 + m(2n+1)$. Ipsum autem residuum medium -1 seu $2n$ sibi ipsum est socium, omnino vti primum $+1$ se ipsum habet pro socio. Reliqua residua

sidua sociata omnia sunt inaequalia, et quocunque proposito r, alterum sibi socium s erit $= \frac{1 + m(2n+1)}{r}$; semper enim m ita definire licet, vt $m(2n+1)+1$ per r diuisionem admittat, siquidem, vti assumimus $2n+1$ fuerit numerus primus, et r numerus ipso minor, vel saltem ad eum primus. Quemadmodum autem in nostra serie residua sunt disposita, cuiusque socium expedite reperitur, cum ambo a medio -1 aequidistent.

Theorema.

44. Si diuisor fuerit numerus quicunque primus P, tot dantur radices primitiuae, quot reperiuntur numeri ad $P-1$ primi eoque minores, quandoquidem tantum radices diuisore minores consideramus.

Demonstratio.

Ponamus $P-1=Q$, et cum certe detur radix primitiua, sit ea $=a$, ita vt a^Q sit minima potestas ipsius a per P diuisa vnitatem relinquens. Tum vero sit n numerus quicunque primus ad Q, ac potestas a^n per diuisorem P diuisa relinquat residuum b, quod vtique ab a erit diuersum; eritque b itidem radix primitiua, seu quod eodem redit ipsa potestas a^n vti radix primitiua spectari potest. Ad quod demonstrandum ostendi debet in progressione Geometrica

$$1,\ a^n,\ a^{2n},\ a^{3n},\ \ldots\ldots\ a^{Qn}$$

ante

ante terminum a^{Qn} nullum occurrere, qui per P diuisus vnitatem relinquat. Iam quia a eſt radix primitiua, nullae aliae eius poteſtates per P diuiſae vnitatem relinquunt, niſi quarum exponentes ſint vel Q, vel 2 Q, vel 3 Q vel multiplum quodcunque ipſius Q, vnde quidem manifeſtum eſt poteſtatem a^{Qn} vnitatem relinquere. Simul vero patet, quia numerus n ad Q eſt primus, nullum multiplum ipſius n minus quam Qn ſimul eſſe multiplum ipſius Q, ſi enim mn exiſtente $m < Q$ eſſet multiplum ipſius Q puta $= kQ$, ob $mn = kQ$ foret $m : Q = k : n$, ideoque numeri n et Q non forent inter ſe primi. Quare cum in ſuperiori progreſſione geometrica ante terminum a^{Qn} nullus alius occurrat, qui per diuiſorem P diuiſus vnitatem relinquat, ſeries reſiduorum inde nata Q terminos diuerſos complectetur eritque propterea completa; et a^n ſeu reſiduum inde natum b erit radix primitiua. Cum igitur ex quolibet numero n ad Q ſeu $P-1$ primo obtineatur radix primitiua, admiſſa vna ſaltem primitiua a, manifeſtum eſt, ſemper tot dari radices primitiuas, quot dantur numeri ad numerum $Q = P - 1$ primi, eoque minores, quandoquidem radices maiores ab hac conſideratione excludimus.

Coroll. 1.

45. Pro diuiſore ergo $P = 3$ et $Q = 2$, vnica datur radix primitiua 2 ex poteſtate a^1 nata; pro diuiſore $P = 5$ et $Q = 4$ duae dantur 2 et 3

ex poteſtatibus a^1 et a^3 natae. Pro diuiſore $P=7$ et $Q=6$, iterum duae dantur 3 et 5 ex poteſtatibus a^1 et a^5 natae. Pro diuiſore $P=11$ et $Q=10$, ad quem numerum Q primi ſunt 1, 3, 7, 9 radices primitiuae ſunt 2, 8, 7, 6 ex poteſtatibus a^1, a^3, a^7, a^9 natae, vti ex ſeriebus reſiduorum completis §. 38. allatis perſpicitur.

Coroll. 2.

46. Pro quouis ergo diuiſore primo P multitudo radicum primitiuarum multitudini numerorum ad numerum $Q=P-1$ primorum eoque minorum eſt aequalis, ideoque ex compoſitione numeri Q eſt iudicanda. Ita ſi fuerit $Q=\alpha^\lambda \beta^\mu \gamma^\nu$ etc. exiſtentibus α, β, γ etc. numeris primis, conſtat numerum radicum primitiuarum fore $=$

$$\alpha^{\lambda-1}(\alpha-1).\ \beta^{\mu-1}(\beta-1).\ \gamma^{\nu-1}(\gamma-1) \text{ etc.}$$

Coroll. 3.

47. Ipſi autem numeri ad Q primi facile reperiuntur, dum ex numeris omnibus ipſo Q minoribus expunguntur ii, qui ad Q ſunt compoſiti: qui enim reſtant, inter quos ſemper vnitas reperitur, erunt ad Q primi.

Scholion.

48. Ex data theorematis demonſtratione autem ſimul intelligitur, plures non dari radices primitiuas, quam aſſignauimus. Sumta enim quacunque alia poteſtate radicis primitiuae iam cognitae a puta a^m, cuius

cuius exponens m non ſit primus ad Q, ſed cum Q communem habeat diuiſorem, qui ſit d, vt tam $\frac{Q}{d}$ quam $\frac{m}{d}$ ſit numerus integer; in progreſſione geometrica $1, a^m, a^{2m}, a^{3m}, a^{4m}$ occurret poteſtas, cuius ſcilicet exponens $= \frac{Q}{d} m$, antequam ad a^{Qm} perueniatur, qui cum ſit quoque $= \frac{m}{d} Q$ ideoque multiplum ipſius Q, ex ea poteſtate iam orietur reſiduum 1, ac propterea ſeries reſiduorum prodibit incompleta. Talis ergo poteſtas a^m ſeu reſiduum inde reſultans certe non erit radix primitiua.

Coroll. 4.

49. Si reſiduum r praebeat radicem primitiuam, etiam eius ſocium s dabit radicem primitiuam. Poſito enim diuiſore primo $P = 2n + 1$ vt ſit $Q = 2n$, ſit $a^{n-\lambda}$ poteſtas praebens reſiduum r, et ſocium s reſultat ex poteſtate $a^{n+\lambda}$. Euidens autem eſt ſi $n - \lambda$ fuerit ad $Q = 2n$ primus, tum etiam exponentem alterum $n + \lambda$ fore ad Q primum.

Scholion.

50. Haud abs re fore arbitror, ſi pro ſimplicioribus diuiſoribus primis P tam numeros ad $Q = P - 1$ primos, quam radices primitiuas iis reſpondentes conſpectui expoſuero:

Diuiſor primus	
3	1 ad 2 primus 2 radix primitiua
5	1, 3 primi ad 4 2, 3 Rad. prim.
7	1, 5 primi ad 6 3, 5 Rad. prim.
11	1, 3, 7, 9 primi ad 10 2, 8, 7, 6 Rad. prim.
13	1, 5, 7, 11 primi ad 12 2, 6, 11, 7 Rad. prim.
17	1, 3, 5, 7, 9, 11, 13, 15 primi ad 16 3, 10, 5, 11, 14, 7, 12, 6 Rad. prim.
19	1, 5, 7, 11, 13, 17 primi ad 18 2, 13, 14, 15, 3, 10 Rad. prim.
23	1, 3, 5, 7, 9, 13, 15, 17, 19, 21 primi ad 22 5, 10, 20, 17, 11, 21, 13, 15, 7. 14 Rad. prim.
29	1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27 primi ad 28 2, 8, 3, 19, 18, 14, 27, 21, 26, 10, 11, 15 Rad. prim.
31	1, 7, 11, 13, 17, 19. 23, 29 primi ad 30 3, 17, 13, 24, 22, 12, 11, 21 Rad. prim.
37	1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35 primi ad 36 2, 32, 17, 13, 15, 18, 35, 5, 20, 24, 22, 19 Rad. prim.

Nullam autem hic inter quemque numerum primum et radices primitiuas ipſi conuenientes relationem deprehendere licet, ex qua pro quouis diuiſore primo ſaltem vnica radix primitiua colligi poſſet;

ſet; atque adeo ordo inter iſtas radices aeque abſconditus videtur, ac inter ipſos numeros primos.

Theorema.

51. Si numeri quadrati per quempiam diuiſorem primum P diuidantur, reſidua inde orta, niſi ſint o, in ſerie reſiduorum completa poteſtatibus parium exponentum reſpondent.

Demonſtratio.

Sit pro diuiſore primo P radix quaedam primitiua a, vt haec progreſſio geometrica

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

ſeriem reſiduorum completam praebeat, in qua omnes numeri diuiſore minores occurrant. Sit iam xx quadratum quodcunque per P diuidendum, et r reſiduum ex diuiſione radicis x ortum, vt ſit $x = mP + r$; ac ſi $r = 0$, ſeu x multiplum diuiſoris P, etiam reſiduum ex quadrato xx natum erit $= 0$, quos caſus, cum per ſe ſint perſpicui, hic non conſideramus. At ſi r ſit numerus quicunque diuiſore P minor, quia in ſerie reſiduorum completa certe continetur, ex certa quadam poteſtate ipſius a, quae ſit a^λ naſcatur neceſſe eſt, tum autem reſiduum ex diuiſione quadrati xx oriundum conueniet cum eo, quod ex diuiſione poteſtatis $a^{2\lambda}$ naſcitur; ſicque ex diuiſione quadratorum alia reſidua reſultare nequeunt, niſi quae ex poteſtatibus formae $a^{2\lambda}$, hoc eſt, quarum exponentes ſunt numeri pares, oriuntur.

 Coroll.

Coroll. 1.

52. Residua ergo, quae ex diuisione quadratorum per diuisorem primum P nascuntur, conuenient cum iis residuis, quae ex hac progressione geometrica nascuntur

$$1, a^2, a^4, a^6, a^8, a^{10}, a^{12} \text{ etc.}$$

existente a radice primitiua.

Coroll. 2.

53. Si ergo diuisor primus sit $P = 2n + 1$, quam formam omnes numeri primi praeter binarium habent, quia 2 non est numerus primus ad $P - 1 = 2n$, etiam a^2 non erit radix primitiua, ideoque series residuorum ex quadratis oriunda non erit completa.

Coroll. 3.

54. Quia autem a^{2n} est minima potestas radicis a vnitatem relinquens, multitudo residuorum, quae ex numeris quadratis resultare possunt, certo est $= n$, cyphra exclusa totidemque numeri nunquam possunt esse residua quadratorum, quos proinde *non-residua* appellaui.

Scholion 1.

55. Hoc etiam ex serie residuorum completa facillime perspicitur, quae si progressioni geometricae subscripta fuerint

$$\begin{array}{l} 1, a, a^2, a^3, a^4, a^5, a^6, a^7 \ldots\ldots a^{2n} \\ 1, \alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta \ldots\ldots 1 \end{array}$$

ex

ex diuiſione quadratorum naſcitur haec ſeries reſiduorum

$$1, \; \epsilon, \; \delta, \; \zeta \; \ldots \ldots \; 1$$

quorum multitudo manifeſto eſt ſemiſſis illorum, quoniam ſerie etiam continuata eadem eodem ordine recurrunt.

Hinc vti reſidua quadratorum ſunt $1, \epsilon, \delta, \zeta$ etc. ita *non-reſidua* erunt $\alpha, \gamma, \varepsilon, \eta$ etc. numero totidem, niſi ſcilicet binarius pro diuiſore primo accipiatur. Quare cum ex ſerie quadratorum $1, 4, 9, 16$ vsque, ad $4nn$ continuata omnia reſidua diuerſa oriri debeant, horumque quadratorum numerus ſit $2n$, reſiduorum vero numerus tantum $= n$, neceſſe eſt ex binis horum quadratorum aequalia reſidua naſci, quod adeo per ſe eſt perſpicuum, cum quadrata bb et $(2n+1-b)^2$ per diuiſorem $2n+1$ diuiſa idem reſiduum relinquant.

Scholion.

56. Simili modo oſtendi poteſt, reſidua, quae ex diuiſione cuborum naſcuntur, non diſcrepare ab iis, quae progreſſioni geometricae $1, a^3, a^6, a^9, a^{12}$ etc. conueniunt, denotante a ſemper radicem primitiuam: Atque in genere ſi poteſtates numerorum quaecunque:

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

per numerum primum P diuidantur, reſidua inde oriunda eadem erunt atque ea, quae ex hac progreſſione geometrica naſcuntur:

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

exiſten-

existente a radice primitiua pro diuisore primo P; vnde patet, si exponens λ fuerit numerus ad $P-1$ primus, seriem residuorum fore completam; at si exponens λ ad $P-1$ non sit primus, ac maximus eorum communis diuisor fuerit $= d$, tum vtique in residuis non omnes numeri occurrent, sed tot tantum, vt eorum multitudo sit $= \frac{P-1}{d}$, cuius ratio ex hactenus allatis satis est manifesta. Sed antequam altiores potestates accuratius scrutemur, quasdam insignes proprietates circa residua quadratorum explicasse iuuabit.

Theorema.

57. Diuisore primo posito $P = 2n + 1$ in residuis quadratorum occurret numerus -1 seu $2n$, quoties n fuerit numerus par; sin autem n sit numerus impar, tum -1 seu $2n$ certe non reperietur in residuis, sed erit *non-residuum*.

Demonstratio.

Cum progressio geometrica $1, a^2, a^4, a^6, a^8$ etc. omnia producat residua quadratorum, euidens est in ea occurrere terminum a^n si quidem n sit numerus par, at supra vidimus potestatem a^n semper dare residuum -1 seu $2n$; ex quo manifestum est, quoties n fuerit numerus par, toties in residuis quadratorum reperiri -1 seu $2n$, contra vero si n fuerit impar, $2n$ seu -1 erit non-residuum.

Coroll.

Coroll. 1.

58. Pro omnibus ergo diuiſoribus primis formae $4n+1$ in reſiduis quadratorum certe occurrit -1 ſeu $4n$, et cum productum ex binis reſiduis iterum ſit reſiduum, ſi reſiduum quodcunque fuerit α, etiam $-\alpha$ in reſiduis reperietur: ſcilicet cuiusque reſidui complementum quoque eſt reſiduum.

Coroll. 2.

59. Pro diuiſoribus autem primis formae $4n-1$, in reſiduis quadratorum certe non occurrit -1 ſed erit *non-reſiduum*; hinc cum productum ex reſiduo et non-reſiduo ſemper ſit *non-reſiduum*, omnium reſiduorum complementa erunt *non-reſidua*.

Theorema.

60 Propoſito numero primo formae $4n+1$ ſemper ſumma duorum quadratorum ad eum primorum exhiberi poteſt, quae ſit per eum diuiſibilis atque alterum quidem quadratum pro lubitu accipere licet.

Demonſtratio.

Sumto enim quadrato quocunque bb, quod per $4n+1$ diuiſum relinquat reſiduum β, dabitur ſemper aliud quadratum xx quod per $4n+1$ diuiſum relinquet reſiduum $-\beta$ ſeu $4n+1-\beta$, ex quo ſumma horum duorum quadratorum $bb+xx$ per numerum primum $4n+1$ diuiſibilis ſit ne-

 ceſſe

cesse est; et cum neutrum per se diuisionem admittat, ea vtique ad $4n+1$ erunt prima.

Coroll. 1.

61. Euidens quoque est quadratum xx infinitis modis accipi posse, cum omnia quadrata in hac forma $(m(4n+1) \pm x)^2$ idem residuum, quod xx praebeant: vnde pro x dabitur valor non solum minor quam $4n+1$, sed etiam minor eius semisse $\frac{4n+1}{2}$ seu minor quam $2n+1$.

Coroll. 2.

62. Semper ergo tales summae binorum quadratorum:

$1+pp$, $4+qq$, $9+rr$, $16+ss$, $25+tt$ etc.

exhiberi possunt, quae omnes sint per numerum primum $4n+1$ diuisibiles; atque ita vt singulorum radices sint minores quum $2n+1$.

Coroll. 3.

63. Cum multitudo numerorum minorum quam $2n+1$ sit $=2n$ ac semper bina quadrata disparia iungantur, multitudo harum formularum erit n: et quia talis summa binorum quadratorum minor est quam $2(2n+1)^2 = 8nn+8n+2$, quotus erit minor quam $2n+\frac{3}{2}$ seu $2n+2$.

Scholion.

64. Quo has summas binorum quadratorum pro quouis numero primo formae $4n+1$ facilius elice-

elicere queamus, residua ex quadratis orta pro simplicioribus apponamus:

num. primi formae $4n+1$	Quadrata 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256 etc. Residua
5	1, −1, −1, 1, 0
13	1, 4, −4, 3, −1, −3, −3, −1, 3, −4, 4, 1, 0
17	1, 4. −8, −1, 8, 2, −2, −4, −4, −2, 2, 8, −1, −8, 4, 1
29	1, 4, 9, −13, −4, 7, −9, 6, −6, 13, 5, −1, −5, −7, −7, −5
37	1, 4, 9, 16, −12, −1, 12, −10, 7, −11, 10, −4, −16, 11, 3, −3, −7, −9, −9.

Hinc pro his diuisoribus formae $4n+1$ sequentes habebimus binorum quadratorum summas per eos diuisibiles:

Diuisor 5 1
$\frac{4}{5}$ quotus 1.

Diuisor 13	1	4	16
	25	9	36
summa	26	13	52
quotus	2	1	4

Diuisor 17 ...	1	4	9	36
	16	64	25	49
summa	17	68	34	85
quotus	1	4	2	5

Diuisor 29 ...	1	4	9	16	36	64	121
	144	25	49	100	196	81	169
summa ..	145	29	58	116	232	145	290
quotus	5	1	2	4	8	5	10

Diuiſor 37 . . .	1	4	9	16	25	64	81	100	225
	36	144	324	169	49	121	289	196	256
ſumma	37	148	333	185	74	185	370	296	481
quotus	2	4	9	5	2	5	10	8	13.

Si igitur demonſtrari poſſet in his quotis ſemper vnitatem reperiri, haberetur demonſtratio completa Theorematis Fermatiani, quod omnis numerus primus formae $4n+1$ ſit ſumma duorum quadratorum. Quoniam vero alibi demonſtraui ſummam duorum quadratorum inter ſe primorum alios diuiſores non admittere, niſi qui ipſi ſint ſummae duorum quadratorum; demonſtratio iam pro abſoluta eſt habenda, quae multo concinnior eſt ea, quam olim per plures ambages elicueram. Sin autem ſimul perpendamus, in quotis illis nullos numeros primos formae $4n-1$ occurrere poſſe, vti mox demonſtrabitur, haec demonſtratio forte multo magis contrahi poterit.

Theorema.

65. Nulla ſumma duorum quadratorum inter ſe primorum per vllum numerum primum formae $4n-1$ diuiſibilis exiſtit.

Demonſtratio.

Quia ſumto quocunque quadrato bb, quod per $4n-1$ diuiſum praebeat reſiduum $\mathfrak{r}$, numerus $-\mathfrak{r}$ ſeu $4n-1-\mathfrak{r}$ ex reſiduis quadratorum prorſus excluditur (58) nullum datur quadratum quod ipſi bb addi-

additum fummam producat per numerum primum $4n-1$ diuifibilem.

Coroll. 1.

66. Summa ergo duorum quadratorum nullum diuiforem admittit formae $4n-1$; etiamfi hic diuifor non fit primus, quoniam tum inter eius factores femper vnus faltem primus formae $4n-1$ contineretur; nifi forte ambo quadrata feorfim per eum fuerint diuifibilia.

Coroll. 2.

67. Quando ergo fumma duorum quadratorum per numerum primum formae $4n+1$ eft diuifibilis, quotus inde refultans neque erit formae $4n-1$, neque vllum habebit factorem primum huius formae, nifi forte ambo quadrata huiusmodi habuerint communem diuiforem, quo cafu quotus adeo quadratum talis numeri contineret.

Coroll. 3.

68. Ex ordine quotorum ergo, qui fupra ex diuifione fummae binorum quadratorum per numerum primum formae $4n+1$ funt orti, excluduntur hi numeri

3, 6, 7, 11, 12, 14, 15, 19, 21, 22, 23, 24, 27, 28, 30, 31 etc.

ac propterea relinquuntur ifti tantum:

1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32 etc.

Problema.

69. Si omnes numeri cubici $1, 2^3, 3^3, 4^3$ etc. per numerum quemcunque primum P diuidantur, inuestigare indolem residuorum, quae inde nascentur.

Solutio.

Sit a radix primitiua respectu diuisoris primi P, et cum progressio geometrica $1, a, a^2, a^3, a^4$ etc. seriem residuorum completam exhibeat, quilibet numerus x per P diuisus idem dabit residuum, quod quaepiam potestas ipsius a quae sit a^λ. Hinc eius numeri cubus x^3 idem dabit residuum quod potestas $a^{3\lambda}$ vnde ex cubis eadem nascentur residua, atque ex progressione geometrica:

$$1, a^3, a^6, a^9, a^{12}, a^{15} \text{ etc.}$$

ac sumto λ ita vt 3λ sit vel $P-1$ vel eius multiplum; potestas $a^{3\lambda}$ vnitatem relinquet. Quare si pro λ minimus numerus accipiatur, cuius triplum fit per $P-1$ diuisibile, numerus λ simul multitudinem omnium residuorum diuersorum, quae ex diuisione cuborum resultare possunt, indicabit.

Cum iam omnis numerus primus sit vel formae $3n+1$ vel $3n+2$, pro vtraque forma iudicium seorsim est instituendum.

I. Sit ergo $P = 3n+1$, et quia $P-1 = 3n$, fiet $\lambda = n$, et residua cuborum omnia ex hac progressione geometrica nascentur:

$$1, a^3, a^6, a^9 \ldots\ldots\ldots a^{3n-3}$$

quia

quia ſequens terminus a^{3n} iterum vnitatem producit. Hinc non plures quam n numeri in reſiduis occurrent ac reliqui duplo plures excluduntur, eruntque non reſidua.

II. Si diuiſor primus ſit $P = 3n + 2$, ideoque $P - 1 = 3n + 1$ minor numerus pro λ accipi nequit, quam $\lambda = 3n + 1$, vt 3λ pro $P - 1$ fiat diuiſibile, vnde omnia reſidua diuerſa ex hac progreſſione geometrica naſcentur:

$$1, a^3, a^6, a^9 \ldots \ldots a^{9n}$$

quorum numerus cum ſit $= 3n + 1$, in reſiduis omnes plane numeri diuiſore P minores occurrent, nullique excluduntur, ſeu nulla dabuntur *non-reſidua*.

Coroll. 1.

70. Si ergo diuiſor primus P fuerit formae $3n + 1$, cuiusmodi numeri ſunt:

7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97 etc.

in reſiduis cuborum tantum n numeri diuerſi occurrunt indeque $2n$ numeri excluduntur.

Coroll. 2.

71. Quare ſi haec cuborum progreſſio

$$1, 2^3, 3^3, 4^3 \ldots \ldots (3n)^3$$

vnde omnia reſidua diuerſa prodire debent, per numerum primum $3n + 1$ diuidantur, quia terminorum numerus eſt $= 3n$, quodlibet reſiduum ter occurrat neceſſe eſt, ſeu ſemper terni cubi, minores

qoum

quam $(3n)^3$, exhiberi possunt qui idem residuum producant.

Scholion. 1.

72. Respectu ergo cuborum numeri primi formae $3n+1$ praecipue notari merentur; operaeque pretium erit residua in casibus simplicioribus notasse:

Diu. pr. $3n+1$	$1, 2^3, 3^3, 4^3, 5^3, 6^3, 7^3, 8^3, 9^3, 10^3, 11^3, 12^3, 13^3, 14^3, 15^3, 16^3, 17^3, 18^3$ Residua
7	$1,\ 1, -1,\ 1, -1, -1,\ 0$
13	$1, -5,\ 1, -1, -5, -5,\ 5,\ 5,\ 1, -1, +5, -1,\ 0$
19	$1,\ 8,\ 8,\ 7, -8,\ 7,\ 1, -1,\ 7, -7,\ 1, -1, -7,\ 8, -7, -8, -8, -1,\ 0$

vbi manifesto quoduis residuum ter occurrit; toties- que idem signo $-$ affectum: cuius ratio inde est perspicua, quod postremus cuiusque ordinis cubus $(3n)^3$ pro residuo dat -1, et producta ex binis residuis semper quoque inter residua reperiantur. Cum migitur praeter cubum $(3n)^3$ semper dentur duo minores pariter residuum -1 habentes, qui sint f^3 et g^3, erunt formulae $1+f^3$ et $1+g^3$ per $3n+1$ diuisibiles, et quia neque $1+f$ neque $1+g$ diuisionem admittit, necesse est vt hae $1-f+ff$ et $1-g+gg$ sint diuisibiles; vbi quidem obseruare licet semper esse debere $g=-ff$ vel $g=m(3n+1)-ff$ quia tum fit $1+g^3=1-f^6$, quae aeque ac $1+f^3$ est diuisibilis.

Scholion 1.

73. Sint f^3, g^3, h^3 terni cubi minores quam $(3n+1)^3$, qui per numerum primum $3n+1$ diuisi

diuisi idem relinquant residuum, et quia binorum differentiae $g^3 - f^3$, $h^3 - f^3$ et $h^3 - g^3$ diuisionem admittunt dum factores $g - f$, $h - f$, $h - g$ diuisore sunt minores, hae tres formae $ff + fg + gg$, $ff + fh + hh$, $gg + gh + hh$ singulae per $3n + 1$ diuisibiles sint necesse est, hincque etiam binarum differentiae $hh - gg + fh - fg = (h - g)(f + g + h)$. Vnde patet quoque summam radicum $f + g + h$ per diuisorem $3n + 1$ esse diuisibilem: quae proprietas illi est analoga, qua inuenimus si bina quadrata ff et gg per numerum quempiam primum P diuisa idem residuum relinquant, dum ambo sunt minora quam P^2, tum summam radicum $f + g$ per P esse diuisibilem. Pro casu nostro trium cuborum erit quoque

$$h(ff+fg+gg)-g(ff+fh+hh)=ff(h-g)-gh(h-g)$$

ideoque formula $ff - gh$ per $3n + 1$ diuisibilis, similique modo $gg - fh$ et $hh - fg$; hinc istas duas formulas ab illa $gg + gh + hh$ auferendo relinquitur haec $fg + fh + gh$ pariter per $3n + 1$ diuisibilis; et haec combinatio $(ff+fg+gg)+(hh-fg)$ praebet hanc $ff + gg + hh$ itidem per $3n + 1$ divisibilem. Quocirca hoc habebimus Theorema satis memorabile.

Theorema.

74. Si f^3, g^3, h^3 fuerint terni cubi minores quam $(3n+1)^3$, qui per numerum primum $3n+1$ diuisi idem relinquant residuum, tum sequentes formulae

$f+g+h$; $fg+fh+gh$; $ff+gg+hh$
singulae diuisionem per $3n+1$ admittent.

Coroll.

75. Ita pro diuisore 19 videmus hos tres cubos 4^3, 6^3 et 9^3 idem residuum 7 dare; vnde ob $f=4$, $g=6$, $h=9$ fit $f+g+h=19$; $fg+fh+gh=114=6.19$ et $ff+gg+hh=133=7.19$.

Theorema.

76. Semper numeri huius formae $pp+3qq$ exhiberi possunt per numerum primum huius formae $3n+1$ diuisibiles. At vero nulla eiusmodi datur formula $pp+3qq$, quae per vllum numerum primum huius formae $3n-1$ sit diuisibilis.

Demonstratio.

Si $3n+1$ est numerus primus, tum tres adeo cubi f^3, g^3, h^3 quorum radices ipso sunt minores, exhiberi possunt, qui per $3n+1$ diuisi idem residuum relinquant; vnde g^3-f^3 per $3n+1$ diuisionem admittet hincque etiam $ff+fg+gg$. At haec forma est vel $(f+\frac{1}{2}g)^2+3(\frac{1}{2}g)^2$ si g sit numerus par, vel $(\frac{1}{2}f+g)^2+3(\frac{1}{2}f)^2$ si f sit par, vel $(\frac{f-g}{2})^2+3(\frac{f+g}{2})^2$, si ambo sint impares, vnde forma $ff+fg+gg$ semper ad hanc $pp+3qq$ reducitur.

At si $3n-1$ sit diuisor primus, omnes cubi, quorum radices ipso sunt minores, diuersa praebent

bent residua, neque ergo binorum differentia, vel numerus huius formae $ff + fg + gg$ exhiberi potest, qui per $3n - 1$ diuidi posset; quod proinde etiam de numeris huius formae $pp + 3qq$ locum habet. Atque hoc adeo de omnibus numeris formae $3n - 1$ valet, quoniam si non fuerint primi, factorem saltem primum istius formae inuoluunt.

Coroll. 1.

77. Si igitur forma $pp + 3qq$ per numerum primum $3n + 1$ sit diuisibilis, et quadratum qq per eundem diuisum relinquat residuum γ, alterum quadratum pp relinquet residuum -3γ. Vnde si omnes numeri quadrati per numerum primum $3n + 1$ diuidantur, in residuis certe reperitur -3 vel $3n - 2$.

Coroll. 2.

78. Sin autem omnes numeri quadrati per numerum primum formae $3n - 1$ diuidantur, in serie residuorum certe non erit numerus -3; ideoque -3 vel $3n - 4$ erit non-residuum.

Scholion.

79. Hinc si numeri quadrati per numerum quemcunque primum diuidantur, de binis numeris $+3$ et -3 iudicari poterit, vtrum in ordine residuorum an *non-residuorum* occurrant. Omnes enim numeri primi praeter 2 et 3 qui hic non spectantur in aliqua harum quatuor formarum continentur:

$$12m + 1 \quad 12m + 5; \quad 12m + 7; \quad 12m + 11$$

quas fingulas contemplemur.

I. Si diuifor primus fit formae $12m+1$, quatenus haec forma eft $4n+1$, tam $+1$ quam -1 erit refiduum; quatenus vero eft $3n+1$, refiduum quoque erit -3, hincque etiam $+3$. Hoc ergo in ordine refiduorum occurrent $+3$ et -3.

II. Si diuifor primus fit formae $12m+5$, quatenus haec forma eft $4n+1$, in refiduis erunt $+1$ et -1; quatenus vero eft $3n-1$ in refiduis non reperitur -3, feu -3 erit non-refiduum, hincque etiam $+3$. Quare hoc cafu neuter numerorum $+3$ et -3 inter refidua reperietur.

III. Si diuifor primus fit formae $12m+7$, quatenus haec forma eft $4n-1$ erit -1 non-refiduum, quatenus vero eft $3n+1$ erit -3 refiduum, ideoque $+3$ non-refiduum. Vnde hoc cafu erit -3 refiduum at $+3$ non-refiduum.

IV. Si diuifor primus fit formae $12m+11$, quatenus haec forma eft $4n-1$, erit -1 non-refiduum, quatenus vero eft formae $3n-1$ erit quoque -3 non-refiduum, vnde $+3$ vtpote productum ex duobus non-refiduis inter refidua occurret. Quare hoc cafu erit $+3$ refiduum at -3 non-refiduum.

Ad hanc ergo egregiam proprietatem confideratio cuborum nos perduxit, quae via cum fatis fit obliqua, alia magis naturalis maxime defideratur.

Proble-

Problema.

80. Si omnes poteſtates quartae per numerum quemcunque primum P diuidantur, inueſtigare indolem reſiduorum, quae inde naſcentur.

Solutio.

Poſita a radice primitiua reſpectu diuiſoris P, vt a^{P-1} ſit infima poteſtas vnitatem relinquens, ac reſidua quaeſita orientur quoque ex hac progreſſione geometrica $1, a^4, a^8, a^{12}, a^{16}$ etc. eousque continuanda, donec exponens per $P-1$ fiat diuiſibilis, quod ſi eueniat in exponente 4λ, erit λ multitudo reſiduorum.

I. Sit diuiſor primus $P = 4n + 1$, vt ſit $P - 1 = 4n$; vnde vt 4λ per $4n$ diuidi queat, erit $\lambda = n$, hocque caſu reſidua quaeſita omnia ex hac progreſſione geometrica naſcentur

$$1,\ a^4,\ a^8,\ a^{12} \ldots\ldots\ldots\ldots a^{4n-4}$$

quorum multitudo eſt n.

II. Sit diuiſor primus $P = 4n + 3$, vt ſit $P - 1 = 4n + 2$; vnde ſumi debet $\lambda = 2n + 1$, et haec progreſſio geometrica

$$1,\ a^4,\ a^8,\ a^{12} \ldots\ldots\ldots\ldots a^{8n}$$

dabit omnia reſidua quaeſita; cum autem a^{4n+2} vnitatem relinquat vti a^0, termini

$$a^{4n+4},\ a^{4n+8},\ a^{4n+12} \text{ etc.}$$

eadem residua praebent atque a^2, a^6, a^{10} etc. vnde his interpolatis oritur progressio

$$1,\ a^2,\ a^4,\ a^6,\ a^8 \ldots\ldots\ldots a^{2n}$$

quae eadem residua dat, ac progressio numerorum quadratorum. Ex biquadratis ergo hoc casu eadem plane residua omnia nascuntur atque ex ipsis quadratis.

Coroll. 1.

81. Si ergo numeri biquadrati per numerum primum formae $4n+1$ diuidantur, tantum n residua diuersa oriuntur, vnde semper quaterna biquadrata dantur p^4, q^4, r^4, s^4, quorum radices diuisore sunt minores, quae per $4n+1$ diuisa idem praebeant residuum; vbi quidem perspicuum est fore $s=-p$ et $r=-q$ seu quod eodem redit $s=4n+1-p$ et $r=4n+1-q$. Hinc istae formulae $p+q+r+s$; $p^2+q^2+r^2+s^2$ et $p^3+q^3+r^3+s^3$ per $4n+1$ erunt diuisibiles.

Coroll. 2.

82. Quaterna ergo biquadrata, quae per numerum primum $4n+1$ diuisa vnitatem relinquent, erunt valores ipsius x, quibus formula x^4-1 per $4n+1$ fit diuisibilis, vnde primo est $x=1$, tum si alius valor sit $x=b$, erit quoque $x=b^2$ et $x=b^3$; neque vltra progredi opus est, quia b^4 vnitati aequiualet.

Coroll. 3.

83. Cum potestas a^{2n} per $4n+1$ residuum det -1, patet si n sit numerus par, in residuis

biqua-

biquadratorum semper reperiri -1, et quoduis residuum quoque signo $-$ affectum occurrere; quod ergo euenit, si diuisor primus sit formae $8m+1$; sin autem sit formae $8m+5$, tum -1 erit nonresiduum.

Coroll. 4.

84. Si ergo diuisor primus sit formae $8m+1$, pro quouis biquadrato b^4 semper dabitur aliud p^4, vt summa b^4+p^4 sit per $8m+1$ diuisibilis, atque adeo quaterna huiusmodi biquadrata p^4 assignari poterunt, quorum radices diuisore sint minores, sin autem diuisor sit formae $8m+5$, tum nulla summa binorum biquadratorum per eum diuisibilis exhiberi potest.

Scholion.

85. Cum summa binorum biquadratorum sit $b^4+p^4=(bb-pp)^2+2(bp)^2$ itemque $b^4+p^4=(bb+pp)^2-2(bp)^2$, pro quouis diuisore primo formae $8m+1$, numeri tam huius formae $xx+2yy$ quam huius $xx-2yy$ exhiberi possunt per $8m+1$ diuisibiles, vnde si numeri quadrati per talem numerum primum $8m+1$ diuidantur, in residuis occurrent numeri $+2$ et -2. Cum igitur demonstrari possit, numeros huius formae $xx+2yy$ alios diuisores non admittere, nisi qui ipsi sint eiusdem formae, hinc sequitur, omnes numeros primos formae $8m+1$ simul in forma $xx+2yy$ contineri. Quod est insigne Theorema Fermatii, cuius demonstrationem nunc primum mihi

hi eruere contigit. Huic autem aliud affine Fermatius proposuit, quod etiam omnes numeri primi huius formae $8m+3$ in eadem forma $xx+2yy$ contineantur, cuius demonstrationem ex hac speculatione petere non licet, sequentem ergo ab amico mecum communicatam hic apponam.

Theorema.

85. Nullus numerus huius formae $2pp-qq$, siquidem p et q sint numeri inter se primi, vllum admittit diuisorem siue huius formae $8m+3$ siue huius $8m-3$.

Demonstratio.

Si numerorum p et q ambo sint impares, numerus $2pp-qq$ habebit formam $8n+1$, sin p sit par et q impar, formam habebit $8n-1$; sin autem p sit impar et q par $=2r$, forma erit $2(pp-2rr)$, ideoque vel $2(8n+1)$ vel $2(8n-1)$; semissis vero $pp-2rr$ iterum in forma $2pp-qq$ continetur, cum sit $pp-2rr=2(p+r)^2-(p+2r)^2$. Hoc praemisso si forma $2pp-qq$ diuisorem haberet $8m\pm3$, per eundem diuisibilis esset numerus formae $8n\pm1$, quotusque ergo foret iterum formae $8m\pm3$, atque minor diuisore; quoniam p et q non solum diuisore, sed etiam eius semisse minores statuere licet. Cum igitur forma $2pp-qq$ per quotum ideoque numerum minorem formae $8m\pm3$ esset diuisibilis, vbi iterum p et q infra eius semissem deprimere licet, quotus denuo minor diuisore orietur, et numeri p et et q ſemper primi inter ſe manerent, ita vt neuter vnquam ad nihilum redigeretur. Tandem ergo ad numerum minimum formae $2pp-qq$ perueniretur, qui foret per numerum formae $8m\pm 3$ hoc eſt vel 3 vel 5 diuiſibilis, quod autem fieri non poſſe per ſe eſt perſpicuum.

Coroll. 1.

87. Quod ſi ergo omnes numeri quadrati per diuiſores primos formae $8m\pm 3$ diuidantur, in reſiduis certe non occurret $+2$, quia alioquin eiusmodi forma $2pp-qq$ diuiſibilis exhiberi poſſet: ideoque pro talibus diuiſoribus erit $+2$ non-reſiduum.

Coroll. 2.

88. Pro diuiſoribus autem primis formae $8m+3$, etiam -1 eſt non-reſiduum, vnde cum producta ex binis non-reſiduis quadratorum tranſeant in reſidua, inter reſidua certe reperietur -2, hincque ſemper numeri formae $2pp+qq$ exhiberi poterunt per numerum primum $8m+3$ diuiſibiles, ex quo numerus primus $8m+3$ ipſe eiusdem formae $2pp+qq$ ſit neceſſe eſt, quod eſt alterum Theorema Fermatii.

Coroll. 3.

89. Pro diuiſoribus autem primis formae $8m-3$, in reſiduis quadratorum reperitur -1, vnde cum productum ex reſiduo in non-reſiduum

ſit non-reſiduum, tam $+2$ quam -2 erunt non-reſidua; ideoque neutra harum formarum $2pp+qq$ et $2pp-qq$ vnquam erit diuiſibilis per vllum numerum primum formae $8m-3$.

Scholion 1.

90. Eodem modo demonſtrari poteſt nullum numerum formae $2pp+qq$, quoniam huiusmodi numeri omnes ſunt vel $8n+1$ vel $8n+3$, per vllos numeros formae vel $8m-1$ vel $8m-3$ eſſe diuiſibiles, quoniam quoti eiusdem forent formae et cum ſint diuiſore minores, perueniendum eſſet ad minores numeros $2pp+qq$ qui forent per $8n-1$ vel $8n-3$ hoc eſt per 7 vel 5 diuiſibiles, quod autem euenire nequit. Hinc porro ſequitur pro diviſoribus primis formae $8m-1$ vel $8m-3$ neceſſario eſſe -2 non-reſiduum: ideoque pro diuiſoribus $8m-1$ erit $+2$ reſiduum, et pro diuiſoribus $8m-3$ non-reſiduum. Quod autem pro diviſoribus primis formae $8m+1$ tam $+2$ quam -2 in reſiduis quadratorum occurrant, ſimili ratiocinio vix oſtendi poſſe videtur.

Scholion 2.

91. Quae hactenus de reſiduis quadratorum ſunt eruta, vtrum numeri ± 2, ac ſupra etiam ± 3 in iis occurrant nec ne? ita conſpectui expoſuiſſe iuuabit:

Diui-

Diuiſor primus

$4n+1$	$+1$	reſiduum
	-1	reſiduum
$4n-1$	$+1$	reſiduum
	-1	non-reſid.
$8n+1$	$+2$	reſiduum
	-2	reſiduum
$8n-1$	$+2$	reſiduum
	-2	non-reſid.
$8n+3$	$+2$	non-reſid.
	-2	reſiduum
$8n-3$	$+2$	non-reſid.
	-2	non-reſid.
$12n+1$	$+3$	reſiduum
	-3	reſiduum
$12n-1$	$+3$	reſiduum
	-3	non-reſid.
$12n+5$	$+3$	non-reſid.
	-3	non-reſid.
$12n-5$	$+3$	non-reſid.
	-3	reſiduum.

Hinc per inductionem vlterius progredi licet hoc modo

Erit	ſi diuiſor primus ſit
$+5$ reſiduum -5 reſiduum	$20n+1$; $20n+9$
$+5$ reſiduum -5 non-reſid.	$20n-1$; $20n-9$

$+5$ non-resid. -5 residuum	$20n+3$; $20n+7$
$+5$ non-resid. -5 non-resid.	$20n-3$; $20n-7$
$+7$ residuum -7 residuum	$28n+1$, -3, 9
$+7$ residuum -7 non-resid.	$28n-1$, $+3$, -9
$+7$ non-resid. -7 residuum	$28n+11$, $+15$, $+23$
$+7$ non-resid. -7 non-resid.	$28n+5$, $+13$, $+17$
$+11$ residuum -11 residuum	$44n+1$, $+9$, $+25$, $+5$, $+37$,
$+11$ residuum -11 non-resid.	$44n-1$, -9, -25, -5, -37,
$+11$ non-resid. -11 residuum	$44n+3$, $+15$, $+23$, $+27$, $+31$,
$+11$ non-resid. -11 non-resid.	$44n+13$, $+17$, $+21$, $+29$, $+41$

quorum Theorematum demonstrationes scientiam numerorum haud mediocriter promouerent.

Theorema.

92. Si omnium numerorum potestates exponentis λ scilicet

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

per

per numerum primum formae $\lambda n + 1$ diuidantur, multitudo reſiduorum diuerſorum erit $= n$, ideoque multitudo non-reſiduorum $= (\lambda - 1) n$.

Demonſtratio.

Sit a radix primitiua pro diuiſore primo $\lambda n + 1$, cuius ergo poteſtates omnia plane ſuppeditant reſidua, et quilibet numerus diuiſore minor x erit reſiduum certae poteſtatis a^m, vnde eius poteſtas x^λ idem praebebit reſiduum quod $a^{\lambda m}$; quare omnia reſidua quaeſita oriuntur ex hac progreſſione geometrica:

$$1,\ a^\lambda,\ a^{2\lambda},\ a^{3\lambda},\ a^{4\lambda} \ldots\ldots a^{(n-1)\lambda}$$

quoniam poteſtas ſequens $a^{\lambda n}$ per numerum primum $\lambda n + 1$ diuiſa iterum vnitatem relinquit, eaque eſt minima hoc praeſtans; ex quo multitudo reſiduorum inde reſultantium eſt $= n$, et cum multitudo omnium numerorum diuiſore minorum ſit $= \lambda n$, reliquorum ex ſerie reſiduorum excluſorum multitudo erit $= (\lambda - 1) n$.

Coroll. 1.

93. Quare ſi ſeries poteſtatum $1, 2^\lambda, 3^\lambda, 4^\lambda$ etc. vsque ad $(\lambda n)^\lambda$ continuetur, in ea ſemper totidem termini, quot exponens λ continet vnitates, reperientur, qui per numerum primum $\lambda n + 1$ diuiſi idem reſiduum relinquant. Totidem ergo erunt qui vnitatem relinquunt, ac ſi vnius radix ſit $= r$, reliquorum radices erunt

$$r^2,\ r^3,\ r^4 \ldots\ldots r^{\lambda - 1}.$$

Coroll. 2.

94. Semper ergo plures huiusmodi numerorum formae $p^\lambda - q^\lambda$ exhiberi possunt per numerum primum $\lambda n + 1$ diuisibiles, ita vt factor $p - q$ non sit diuisibilis; atque adeo alterum numerorum p et q pro lubitu accipere licet.

Coroll. 3.

95. Si n sit numerus par, in progressione geometrica $1, a^\lambda, a^{2\lambda}$ etc. occurret terminus $a^{\frac{1}{2} n \lambda}$, cui residuum -1 respondet; quare si diuisor primus sit $2m\lambda + 1$ in residuis reperietur -1, sin autem sit $(2m+1)\lambda + 1$ tum -1 erit non-residuum: euidens autem est si λ sit numerus impar, posteriorem formam locum habere non posse.

Scholion 1.

96. Si omnes numerorum potestates quaesitae $1, 2^5, 3^5, 4^5$ etc. per numeros primos formae $5n + 1$ qui sunt: 11, 31, 41, 61, 71 etc. diuidantur, tantum n residua diuersa resultabunt, inter quae vtique reperietur -1. Huiusmodi ergo numerorum formae $p^5 \pm q^5$ dabuntur per numerum primum $5n + 1$ diuisibiles, ita factor $p \pm q$ diuisionem non admittat. Hinc alter factor qui est $p^4 \mp p^3 q + p^2 q^2 \mp p q^3 + q^4$ per eundem erit diuisibilis, qui cum sit $(pp \pm \frac{1}{2} pq + qq)^2 - 5(\frac{1}{2} pq)^2$, dabitur huiusmodi forma $ff - 5gg$ per $5n + 1$ diuisibilis; vnde sequitur si quadrata diuidantur per numerum primum formae $5n + 1$, tum inter residua certe repe-

reperiri $+5$, quod cum coniectura ante allata congruit.

Scholion 2.

97. Simili modo si potestates septimae per numerum primum $7n+1$ diuidantur, dabuntur huiusmodi formae $p^7 - q^7$ seu $p^6 + p^5 q + p^4 q^2 + p^3 q^3 + p^2 q^4 + p q^5 + q^6$ per eum diuisibiles; haec vero expressio reducitur ad hanc formam:

$$(p^3 + \tfrac{1}{2}ppq - \tfrac{1}{2}pqq - q^3)^2 + 7(\tfrac{1}{2}ppq + \tfrac{1}{2}pqq)^2.$$

Vnde semper numeri huius formae $ff + 7gg$ exhiberi possunt per numerum primum $7n+1$ diuisibiles. Ex quo sequitur si omnia quadrata per numerum primum formae $7n+1$ diuidantur inter residua certe repertum iri -7, quo etiam coniectura supra data confirmatur.

NOVA