mi possit, residua minima numerorum a, aa, a^3 .... a^d (quae omnia sunt diuersa) esse radices congruentiae $x^d \equiv 1$, haec autem plures quam d radices diuersas habere nequeat, manifestum est, praeter numerorum a, aa, a^3 .... a^d residua minima alios numeros inter 1 et $p-1$ incl. non dari quorum potestates exponentis d congruae sint vnitati. Hinc patet omnes numeros ad exponentem d pertinentes inter residua minima numerorum a, aa, a^3 .... a^d reperiri. Quales vero sint, quantaque eorum multitudo ita definitur. Si k est numerus ad d primus, omnes potestates ipsius a^k, quarum exponentes $< d$, vnitati non erunt congrui: esto enim $\frac{1}{k}$ (mod. d) $\equiv m$ (vid. art. 31) eritque $a^{km} \equiv a$; quare si potestas e^{ta} ipsius a^k vnitati esset congrua atque $e < d$, foret etiam $a^{kme} \equiv 1$ et hinc $a^e \equiv 1$ contra hyp. Hinc manifestum est, residuum minimum ipsius a^k ad exponentem d pertinere. Si vero k diuisorem aliquem, δ, cum d communem habet, ipsius a^k residuum minimum ad exponentem d non pertinet; quoniam tum potestas $\frac{d}{\delta}^{ra}$ iam vnitati fit congrua (erit enim $\frac{kd}{\delta}$ per d diuisibilis, siue $\equiv 0$ (mod. d) adeoque $a^{\frac{kd}{\delta}} \equiv 1$). Hinc colligitur, totidem numeros ad exponentem d pertinere quot numerorum 1, 2, 3 .... d ad d sint primi. At memorem esse oportet, hanc conclusionem innixam esse suppositioni, vnum numerum a iam haberi ad exponentem d pertinentem. Quamobrem dubium remanet, fierine possit vt ad aliquem exponentem nullus omnino numerus pertineat; conclusioque eo limitatur vt ψd sit vel $= 0$ vel $= \varphi d$.

54. II. Iam sint omnes diuisores numeri $p-1$ hi: d, d', d'', etc. eritque, quia omnes numeri $1, 2, 3 \ldots\ldots p-1$ inter hos sunt distributi, $\psi d + \psi d' + \psi d'' +$ etc. $= p-1$. At in art. 40 demonstrauimus esse $\varphi d + \varphi d' + \varphi d'' +$ etc. $= p-1$, atque ex art. praec. sequitur ψd ipsi φd aut aequalem aut ipso minorem esse, maiorem esse non posse, similiterque de $\psi d'$ et $\varphi d'$, etc. Si itaque aliquis terminus ex his ψd, $\psi d'$, $\psi d''$ etc. termino respondente ex his φd, $\varphi d'$, $\varphi d''$, esset minor (siue etiam plures) illorum summa summae horum aequalis esse non posset. Vnde tandem concludimus *ψd ipsi φd semper esse aequalem*, adeoque a magnitudine ipsius $p-1$ non pendere.

55. Maximam autem attentionem meretur casus particularis propositionis praecedentis scilicet *semper dari numeros quorum nulla potestas inferior quam $p-1^{ta}$ vnitati congrua*, et quidem totidem inter 1 et $p-1$ quot infra $p-1$ sint numeri ad $p-1$ primi. Cuius theorematis demonstratio quum minime tam obuia sit quam primo aspectu videri possit, propter theorematis dignitatem liceat aliam adhuc adiicere a praecedente aliquantum diuersam, quandoquidem methodorum diuersitas ad res obscuriores illustrandas plurimum conferre solet. Resoluatur $p-1$ in factores suos primos fiatque $p-1 = a^\alpha b^\beta c^\gamma$ etc., designantibus a, b, c etc. numeros primos inaequales. Tum theorematis demonstrationem per sequentia absoluemus:

I. Semper inueniri posse numerum A, (aut plures), ad exponentem a^α pertinentem, similiterque numeros B, C etc. ad exponentes b^{ε}, c^{γ} etc. respectiue pertinentes.

II. Productum ex omnibus numeris A, B, C etc. (siue huius producti residuum minimum) ad exponentem $p-1$ pertinere. Haec autem ita demonstramus.

I. Sit g numerus aliquis ex his $1, 2, 3 \ldots p-1$, congruentiae $x^{\frac{p-1}{a}} \equiv 1$ (mod. p) *non* satisfaciens, omnes enim hi numeri congruentiae huic, cuius gradus $< p-1$, satisfacere nequeunt. Tum dico si potestas $\frac{p-1}{a^{\alpha}}$ ta ipsius g ponatur $\equiv h$, hunc numerum, siue eius residuum minimum ad exponentem a^{α} pertinere.

Namque patet potestatem a^{α} tam ipsius h congruam fore potestati $p-1$ tae ipsius g *i. e.* vnitati, potestas vero $a^{\alpha-1}$ta ipsius h congrua erit potestati $\frac{p-1}{a}$ tae ipsius g, *i. e.* vnitati erit incongrua, multoque minus potestates $a^{\alpha-2}$, $a^{\alpha-3}$ tae etc. ipsius h vnitati congruae esse possunt. At exponens infimae potestatis ipsius h, vnitati congruae, siue exponens ad quem pertinet h, numerum a^{α} metiri debet (art. 48). Quare quum a^{α} per alios numeros diuisibilis non sit quam per se ipsum, atque per inferiores ipsius a potestates, necessario a^{α} erit exponens ad quem h pertinet. *Q. E. D.* Per similem methodum demonstratur, dari numeros ad exponentes b^{ε}, c^{γ} etc. pertinentes.

II. Si supponimus, productum ex omnibus A, B, C etc. non ad exponentem $p-1$, sed ad minorem t pertinere, t ipsum $p-1$ metietur (art. 48), siue erit $\frac{p-1}{t}$ integer vnitate maior. Facile autem perspicitur, hunc quotientem vel