1) Si duorum numerorum vel summa vel differentia per 2^{n-1} est diuisibilis, numerorum quadrata erunt congrua secundum modulum 2^n. Si enim alter ponitur $= a$, erit alter formae $2^{n-1}h \pm a$, cuius quadratum inuenitur $\equiv aa$ (mod. 2^n).

2) Quiuis numerus impar, qui ipsius 2^n est residuum quadraticum, congruus erit quadrato alicui, cuius radix est numerus impar et $< 2^{n-2}$ Sit enim quadratum quodcunque cui numerus ille congruus, aa atque numerus $a \equiv \pm \alpha$ (mod. 2^{n-1}) ita vt α moduli semissem non superet (art. 4), eritque $aa \equiv \alpha\alpha$. Quare etiam numerus propositus erit $\equiv \alpha\alpha$. Manifesto vero tum a tum α erunt impares atque $\alpha < 2^{n-2}$.

3) Omnium numerorum imparium ipso 2^{n-2} minorum quadrata secundum modulum 2^n incongrua erunt, Sint enim duo tales numeri r et s, quorum quadrata si secundum 2^n essent congrua, foret $(r-s)(r+s)$ per 2^n diuisibilis (posito $r > s$). Facile vero perspicitur numeros $r-s$, $r+s$, simul per 4 diuisibiles esse non posse, quare si alter tantummodo per 2 est diuisibilis, alter vt productum per 2^n diuisibilis fieret, per 2^{n-1} diuisibilis esse deberet, *Q. E. A.* quoniam vterque $< 2^{n-1}$.

4) Quodsi denique haec quadrata ad *residua* sua *minima positiua* reducuntur, habebuntur 2^{n-3} residua quadratica diuersa modulo minora, quorum quoduis erit formae $8k+1$.

Sed quum praecise 2^{n-3} numeri formae $8k+1$ modulo minores exstent, necessario hi omnes inter illa residua reperientur. *Q. E. D.*

Vt quadratum numero dato formae $8k+1$ secundum modulum 2^n congruum inueniatur, methodus similis adhiberi potest, vt in art. 102; vid. etiam art. 88. — Denique de numeris paribus eadem valent, quae art. 102 generaliter exposuimus.

104. Circa multitudinem valorum diuersorum (i. e. secundum modulum incongruorum), quos expressio talis $V \equiv \sqrt{A}(\text{mod. } p^n)$ admittit, siquidem A est residuum ipsius p^n, facile e praecc. colliguntur haec. (Numerum p supponimus esse primum, vt ante, et breuitatis caussa casum $n = 1$ statim includimus). I. Si A per p non est diuisibilis, V *vnum* valorem habet pro $p = 2$, $n = 1$, puta $V \equiv 1$; *duos*, quando p est impar, nec non pro $p = 2$, $n = 2$, puta ponendo vnum $\equiv v$, alter erit $\equiv -v$; *quatuor* pro $p = 2$, $n > 2$, scilicet ponendo vnum $\equiv v$, reliqui erunt $\equiv -v$, $2^{n-2}+v$, $2^{n-2}-v$. II. Si A per p diuisibilis est, neque vero per p^n, sit potestas altissima ipsius p ipsum A metiens $p^{2\mu}$ (manifesto enim ipsius exponens par esse debebit) atque $A = ap^{2\mu}$. Tunc patet, omnes valores ipsius V per p^μ diuisibiles esse, et quotientes e diuisione ortos fieri valores expr. $V' \equiv \sqrt{a}(\text{mod. } p^{n-2\mu})$; hinc omnes valores diuersi ipsius V prodibunt, multiplicando omnes valores expr. V' inter 0 et $p^{n-\mu}$ sitos per p^μ; quare illi exhibebuntur per vp^μ, $vp^\mu + p^{n-\mu}$, $vp^\mu + 2p^{n-\mu} \ldots vp^\mu + (p^\mu - 1)p^{n-\mu}$,

si v indefinite omnes valores *diuersos* expr. V exprimit, ita vt illorum multitudo fiat p^{μ}, $2p^{\mu}$ vel $4p^{\mu}$, prout multitudo horum (per casum I) est 1, 2 vel 4. III. Si A per p^{n} diuisibilis est, facile perspicietur, statuendo $n = 2m$ vel $= 2m - 1$, prout par est vel impar, omnes numeros per p^{m} diuisibiles, neque vllos alios, esse valores ipsius V; quare omnes valores diuersi hi erunt 0, p^{m}, $2p^{m} \ldots (p^{n-m} - 1)p^{m}$, quorum multitudo p^{n-m}.

105. Superest casus, vbi modulus m e pluribus numeris primis compositus est. Sit $m = abc\ldots$, designantibus a, b, c etc. numeros primos diuersos aut primorum diuersorum potestates, patetque statim, si n sit residuum ipsius m, fore etiam n residuum singulorum a, b, c etc., adeoque n certo nonresiduum ipsius m esse, si fuerit NR. vllius e numeris a, b, c etc. Vice versa autem, si n singulorum a, b, c etc. residuum est, etiam residuum producti m erit. Supponendo enim, $n \equiv A^2$, B^2, C^2 etc. sec. mod. a, b, c etc. resp., patet, si numerus N ipsis A, B, C etc. sec. mod. a, b, c etc. resp. congruus eruatur (art. 32), fore $n \equiv NN$ secundum omnes hos modulos adeoque etiam secundum productum m. — Quum facile perspiciatur, hoc modo e combinatione *cuiusuis* valoris ipsius A siue expr. $\sqrt{n}$ (mod. a) cum *quouis* valore ipsius B cum *quouis* valore ipsius C etc. oriri valorem ipsius N siue expr. $\sqrt{n}$ (mod. m), nec non e combinationibus diuersis produci diuersos N, et e cunctis cunctos: multitudo omnium valorum diuersorum ipsius N aequalis