modulique semisse minorum quadrata essent congrua, foret $aa - bb$ siue $(a - b)(a + b)$ per p^n diuisibilis (posito i. q. licet $a > b$) Hoc vero fieri non potest, nisi *vel* alter numerorum $a - b$, $a + b$ per p^n fuerit diuisibilis, quod fieri nequit, quoniam vterque $< p^n$, *vel* alter per p^m alter vero per $p^{n-\mu}$, i. e. vterque per p. Sed etiam hoc fieri nequit. Manifesto enim etiam summa et differentia $2a$ et $2b$ per p foret diuisibilis adeoque etiam a et b contra hyp. — Hinc tandem colligitur inter numeros per p non diuisibiles moduloque minores $\frac{1}{2}(p - 1)p^n$ residua dari, reliquos quorum multitudo aeque magna, esse non-residua *Q. E. D.* — Potest etiam theorema hoc ex consideratione indicum deriuari simili modo vt art. 97.

101. *Quiuis numerus per p non diuisibilis, qui ipsius p est residuum, erit residuum etiam ipsius p^n; qui vero ipsius p est non-residuum, etiam ipsius p^n non-residuum erit.*

Pars posterior huius propositionis per se est manifesta. Si itaque prior falsa esset, inter numeros ipso p^n minores simulque per p non diuisibiles plures forent residua ipsius p, quam ipsius p^n, *i. e.* plures quam $\frac{1}{2}p^{n-1}(p - 1)$. Nullo vero negotio perspici poterit, multitudinem residuorum numeri p inter illos numeros esse praecise $= p^{n-1}(p - 1)$.

Aeque facile est, quadratum reipsa inuenire, quod secundum modulum p^n residuo dato sit congruum, si quadratum huic residuo secundum modulum p congruum habetur.

Scilicet si quadratum habetur, aa, quod residuo dato A secundum modulum p^μ est congruum, deducitur inde quadratum ipsi A secundum modulum p^ν congruum (vbi $\nu > \mu$ et $=$ vel $< 2\mu$ supponitur) sequenti modo. Ponatur radix quadrati quaesiti $= \pm a + xp^\mu$, quam formam eam habere debere facile perspicitur; debetque esse $aa \pm 2axp^\mu + xxp^{2\mu} \equiv A \pmod{p^\nu}$ siue propter $2\mu > \nu$, $A - aa \equiv \pm 2axp^\mu \pmod{p^\nu}$ Sit $A - aa = p^\mu d$, eritque, x valor expressionis $\pm \frac{d}{2a} \pmod{p^{\nu-\mu}}$ quae huic $\pm \frac{A - aa}{2ap^\mu} \pmod{p^\nu}$ aequiualet.

Dato igitur quadrato ipsi A secundum p congruo, deducitur inde quadratum ispi A secundum modulum p^2 congruum; hinc ad modulum p^4, hinc ad p^8 etc. ascendi poterit.

Ex. Proposito residuo 6, quod secundum modulum 5 quadrato 1 congruum, inuenitur quadratum 9^2 cui secundum 25 est congruum, 16^2 cui secundum 125 congruum etc.

102. Quod vero attinet ad numeros per p diuisibiles, patet, eorum quadrata per pp fore diuisibilia, adeoque omnes numeros per p quidem diuisibiles, neque vero per pp, ipsius p^n fore non residua. Generaliter vero, si proponitur numerus p^kA vbi A per p non est diuisibilis, hi casus erunt distinguendi:

1) Quando $k =$ vel $> n$, erit $p^kA \equiv o \pmod{p^n}$, i. e. residuum.

2) Quando $k < n$ atque impar, erit p^kA non residuum.

Si enim esset $p^k A \equiv p^{2\varkappa+1} A \equiv ss \pmod{p^n}$, ss per $p^{2\varkappa+1}$ diuisibilis esset, id quod aliter fieri nequit, quam si fuerit s per $p^{2\varkappa+1}$ diuisibilis. Tunc vero ss etiam per $p^{2\varkappa+2}$ diuisibilis, adeoque etiam (quia $2^\varkappa + 2$ certo non maior quam n) $p^k A$, i. e. $p^{2\varkappa+1} A$; siue A per p, contra hyp.

3) Quando $k < n$ atque par. Tum $p^k A$ erit residuum vel non-residuum ipsius p^n, prout A est residuum vel non-residuum ipsius p. Quando enim A est residuum ipsius p, erit etiam residuum ipsius p^{n-k}. Posito autem $A \equiv aa \pmod{p^{n-k}}$ erit $Ap^k \equiv aap^k \pmod{p^n}$ aap^k vero est quadratum. Quando autem A est non-residuum ipsius p, $p^k A$ residuum ipsius p^n esse nequit. Ponatur enim $p^k A \equiv aa \pmod{p^n}$, eritque necessario aa per p^k diuisibilis. Quotiens erit quadratum cui A secundum modulum p^{n-k} adeoque etiam secundum modulum p congruus, i. e. A erit residuum ipsius p contra hyp.

103. Quoniam casum $p = 2$ exclusimus, de hoc adhuc quaedam dicenda. Quando numerus 2 est modulus, numerus quicunque erit residuum, non-residua nulla erunt. Quando vero 4 est modulus, omnes numeri impares formae $4k+1$ erunt residua, omnes vero formae $4k+3$ non-residua. Tandem quando 8 aut altior potestas numeri 2 est modulus, omnes numeri impares formae $8k+1$ erunt residua, reliqui vero, seu ii qui sunt formarum $8k+3$, $8k+5$, $8k+7$, erunt non-residua. Pars posterior huius propositionis inde clara, quod quadratum cuiusuis numeri imparis, siue sit formae $4k+1$, siue formae $4k-1$, fit formae $8k+1$. Priorem ita probamus.