4, 9.... $(\frac{1}{2}m)^2$ congrui sint, quadrato congruos fieri non posse, quando m par; quando vero impar, quemuis numerum, qui vlli quadrato sit congruus, alicui ex his 0, 1, 4, 9... $(\frac{1}{2}m - \frac{1}{2})^2$ necessario congruum esse. Quare dabuntur ad summum in priori casu $\frac{1}{2}m + 1$ residua minima diuersa, in posteriori $\frac{1}{2}m + \frac{1}{2}$ *Q. E. D.*

95. *Exemplum.* Secundum modulum 13 quadratorum numerorum 0, 1, 2, 3... 6 residua minima inueniuntur, 0, 1, 4, 9, 3, 12, 10, post haec vero eadem ordine inuerso recurrunt 10, 12, 3, etc. Quare numerus quisque, nulli ex istis residuis congruus, siue qui alicui ex his est congruus, 2, 5, 6, 7, 8, 11, nulli quadrato congruus esse potest.

Secundum modulum 15 haec inueniuntur residua, 0, 1, 4, 9, 1, 10, 6, 4 post quae eadem ordine inuerso recurrunt. Hic igitur numerus residuuorum, quae quadrato congrua fieri possunt, minor adhuc est, quam $\frac{1}{2}n + \frac{1}{2}$, quum sint 0, 1, 4, 6, 9, 10. Numeri autem 2, 3, 5, 7, 8, 11, 12, 13, 14, et qui horum alicui sunt congrui, nulli quadrato secundum mod. 15 congrui fieri possunt.

96. Hinc colligitur, pro quouis modulo omnes numeros in duas classes distingui posse, quarum altera contineat numeros, qui quadrato alicui congrui fieri possint, altera eos qui non possint. Illos appellabimus *residua quadratica*

numeri istius quem pro modulo accepimus *), hos vero *ipsius non-residua quadratica*, siue etiam, quoties ambiguitas nulla inde oriri potest, simpliciter *residua* et *non-residua*. Ceterum palam est sufficere, si omnes numeri 0, 1, 2... $m-1$ in classes redacti sint: numeri enim congrui ad eandem classem erunt referendi.

Etiam in hac disquisitione a modulis primis initium faciemus, quod itaque subintelligendum erit, etiamsi expressis verbis non moneatur. Numerus primus 2 autem excludendus, siue numeri primi *impares* tantum considerandi.

96. *Numero primo p pro modulo accepto, numerorum* 1, 2, 3.... $p-1$ *semissis erunt residua quadratica, reliqui non-residua, i. e. dabuntur* $\frac{1}{2}(p-1)$ *residua, totidemque non-residua.*

Facile enim probatur, omnia quadrata 1, 4, 9... $\frac{1}{2}(p-1)^2$ esse incongrua. Scilicet si fieri posset $rr \equiv r'r'$ (mod. p) atque numeri r, r' inaequales et non maiores quam $\frac{1}{2}(p-1)$ posito $r > r'$ i. q. licet, fieret $(r-r')(r+r')$ positiuus et per p diuisibilis. At vter-

*) Proprie quidem hic casu secundo alio sensu vtimur, quam hucusque fecimus. Dicere scilicet oporteret, r esse residuum quadrati aa secundum modulum m quando $r \equiv aa$ (mod. m); at breuitatis gratia in hac sectione semper r *ipsius* m residuum quadraticum vocamus, neque hinc vlla ambiguitas metuenda. Expressionem enim, *residuum*, quando idem significat quod numerus congruus, abhinc non adhibebimus, nisi forte de residuus *minimis* sermo sit, vbi nullum dubium esse potest.

que factor $r - r'$, et $r + r'$ ipso p est minor, quare suppositio consistere nequit (art. 13). Habentur itaque $\frac{1}{2}(p-1)$ residua quadratica, inter hos numeros $1, 2, 3 \ldots p-1$ contenta; plura vero inter ipsos esse nequeunt quia accedente residuo oprodeunt $\frac{1}{2}(p+1)$, quem numerum omnium residuorum multitudo superare nequit. Quare reliqui numeri erunt non residua horumque multitudo $= \frac{1}{2}(p-1)$.

Quum cifra semper sit residuum, hanc numerosque per modulum diuisibiles ab inuestigationibus his excludimus, quia hic casus per se est clarus, theorematumque concinnitatem tantum turbaret. Ex eadem caussa etiam modulum 2 exclusimus.

97. Quum plura quae in hac Sect. exponemus etiam ex principiis Sect. praec. deriuari possint, neque inutile sit, eandem veritatem per methodos diuersas perscrutari, hunc nexum ostendemus. Facile vero intelligitur, omnes numeros quadrato congruos, indices *pares* habere, eos contra, qui quadrato nullo modo congrui fieri possint, impares. Quia vero $p-1$ est numerus par, tot indices pares erunt quot impares, scilicet $\frac{1}{2}(p-1)$, totidemque tum residua tum non residua dabuntur.

Exempla.

Pro modulis sunt residua

3 . . . . . 1.
5 . . . . . 1, 4.