(III) designabitur) totidem ad minimum termini erunt secundum modulum p ipsi r congrui, quot in serie (II) per p diuisibiles (art. praec.). Inter illos autem, bini, qui signo tantum, non magnitudine, discrepent, occurrere nequeunt*). Tandem quisque eorum correspondentem habebit in serie (I), qui per p erit diuisibilis. Scilicet si fuerit $\pm b$ aliquis terminus seriei (III) ipsi r secundum p congruus, erit $a - bb$ per p diuisibilis. Quodsi igitur b est par, terminus seriei (I), $2(a - bb)$, per p diuisibilis erit. Si vero b impar, terminus $\frac{1}{2}(a - bb)$ per p diuisibilis erit: namque manifesto $\frac{a-bb}{p}$ erit integer *par*, quoniam $a - bb$ per 8, p autem ad summum per 4 diuisibilis (a enim per hyp. est formae $8n + 1$, bb autem ideo quod est numeri imparis quadratum eiusdem formae erit, quare differentia erit formae $8n$). Hinc tandem concluditur, in serie (I) totidem terminos esse per p diuisibiles, quot in (III) sint ipsi r secundum p congrui, *i. e.* totidem aut plures quam in (II) sint per p diuisibiles. *Q. E. D.*

III. Sit p formae $8n$, atque $a \equiv rr$ (mod. $2p$). Facile enim perspicitur, a, quum ex hyp. ipsius p sit residuum, etiam ipsius $2p$ residuum

*) Si enim esset $r \equiv -f \equiv +f$ (mod. p), fieret $2f$ per p diuisibilis, adeoque etiam $2a$ (propter $ff \equiv a$ (mod. p)) Hoc autem aliter fieri nequit, quam si $p = 2$, quum per hyp. a ad p sit primus. Sed de hoc casu iam seorsim diximus.

fore. Tum in serie (III) totidem ad minimum termini erunt ipsi r secundum p congrui quot in (II) sunt per p diuisibiles, illique omnes magnitudine erunt inaequales. At cuique eorum respondebit aliquis in (I) per p diuisibilis. Si enim $+b$ vel $-b \equiv r$ (mod. p), erit $bb \equiv rr$ (mod. $2p$), *) adeoque terminus $\frac{1}{2}(a-rr)$ per p diuisibilis, multoque magis $2(a-rr)$. Quare in (I) totidem ad minimum termini erunt per p diuisibiles quam in (II). *Q. E. D.*

129. Theorema. *Si a est numerus primus formae $8n+1$, necessario infra $2\sqrt{a}$ dabitur aliquis numerus primus cuius non-residuum sit a.*

Demonstr. Esto, si fieri potest, a residuum omnium primorum ipso $2\sqrt{a}$ minorum. Tum facile perspicietur, a etiam omnium numerorum compositorum ipso $2\sqrt{a}$ minorum residuum fore (conferantur praecepta per quae diiudicare docuimus, vtrum numerus propositus sit numeri compositi residuum necne; art. 105). Sit numerus proxime minor quam $\sqrt{a} = m$. Tum in serie (I)..... a, $\frac{1}{2}(a-1)$, $2(a-4)$, $\frac{1}{2}(a-9)$.... $2(a-mm)$, vel $\frac{1}{2}(a-mm)$, totidem aut plures termini erunt per numerum quemcunque ipso $2\sqrt{a}$ minorem diuisibiles, quam in hac (II)..... 1, 2, 3, 4.... $2m+1$ (art. praec.). Hinc vero sequitur, productum ex omnibus terminis (I) per productum omnium terminorum (II) diuisibile

*) Erit scilicet $bb - rr = (b-r)(b+r)$ e duobus factoribus compositus, quorum alter per p diuisibilis (hyp.), alter per 2 (quia tum b tum r sunt impares); adeoque $bb - rr$ per $2p$ diuisibilis.

esse, (art. 126). At illud est aut $= a (a - 1) (a - 4) \ldots (a - mm)$ aut semissis huius producti (prout m aut par aut impar). Quare productum $a(a - 1)(a - 4) \ldots (a - mm)$ certo per productum omnium terminorum (II) diuidi poterit, et, quia omnes hi termini ad a sunt primi, etiam productum illud omisso factore a. Sed productum ex omnibus terminis (II) ita etiam exhiberi potest, $(m + 1) \cdot ((m + 1)^2 - 1) . ((m + 1)^2 - 4) \ldots ((m + 1)^2 - m^2)$. Fiet igitur

$$\frac{1}{(m+1)^2} \cdot \frac{a - 1}{(m + 1)^2 - 1} \cdot \frac{a - 4}{(m + 1)^2 - 4} \cdots \frac{a - m^2}{(m+1)^2 - m^2}$$

numerus integer, quamquam sit productum ex fractionibus vnitate minoribus: quia enim necessario $\sqrt{a}$ irrationalis esse debet; erit $m + 1 > \sqrt{a}$, adeoque $(m + 1)^2 > a$. Hinc tandem concluditur suppositionem nostram locum habere non posse. *Q. E. D.*

Iam quia a certo > 4, erit $2 \sqrt{a} < a$, dabiturque adeo aliquis primus $< a$ cuius non-residuum a.

130. Postquam rigorose demonstrauimus quemuis numerum primum formae $4n + 1$, et positiue et negatiue acceptum, alicuiuis numeri primi ipso minoris non-residuum esse, ad comparationem exactiorem et generaliorem numerorum primorum quatenus vnus alterius residuum vel non-residuum est, statim transimus.

Omni rigore supra demonstrauimus, $- 3$ et $+ 5$ esse residua vel non-residua omnium numerorum primorum, qui ipsorum 3, 5 respectiue sint residua vel non-residua.