quarum quaeuis bina residua socia contineat. Iam perspicuum est, si nullum residuum daretur, quod sibi ipsi esset socium, i. e. si quaeuis classis bina residuae *inaequalia* contineret, omnium residuorum numerum fore duplum numeri omnium classium; quodsi vero aliqua dantur residua sibi ipsis socia, i. e. aliquae classes quae vnicum tantum residuum aut, si quis malit, idem residuum bis continent, posita harum classium multitudine $= a$, reliquarumque multitudine $= b$; erit omnium residuorum C numerus $= a + 2b$. Quare quando p est formae $4n + 1$, erit a numeros par; quando autem p est formae $4n + 3$, erit a impar. At numeri ipso p minores alii, quam 1 et $p - 1$, sibi ipsis socii esse nequeunt (vid. art. 77); priorque 1 certo inter residua occurrit; vnde in priori casu $p - 1$ (seu quod hic idem valet, -1) debet esse residuum, in posteriori vero non-residuum; alias enim in illo casu foret $a = 1$, in hoc autem $= 2$, quod fieri nequit.

110. Etiam haec demonstratio ill. Eulero debetur, qui et priorem primus inuenit. V. *Opusc. Anal.* T. I. *p* 135. — Facile quisquis videbit eam similibus principiis innixam esse, vt demonstratio nostra secunda theor. Wilsoniani art. 77. Si vero hoc theorema supponere velimus, facilius adhuc demonstratio exhiberi poterit. Scilicet inter numeros 1, 2, 3... $p - 1$ erunt $\frac{p-1}{2}$ residua quadratica ipsius p totidemque non-residua; quare non-residuorum multitudo erit par, quando p est formae $4n + 3$. Hinc productum ex omnibus numeris

1, 2, 3 . . . $p - 1$ in priori casu erit residuum, in posteriori non-residuum (art. 99). At productum hoc semper $\equiv -1 \pmod{p}$; adeoque etiam -1 in priori casu residuum, in posteriori non-residunm erit.

111. Si itaque r est residuum numeri alicuius primi formae $4n + 1$, etiam $-r$ huius primi residuum erit, omnia autem talis numeri non-residua, etiam signo contrario sumta non-residua manebunt. Contrarium euenit pro numeris primis formae $4n + 3$, quorum residua quando signum mutatur, non-residua fiunt et vice versa, vid. art. 98.

Ceterum facile ex praecadentibus deriuatur regula generalis: -1 residuum omnium numerorum qui neque per 4 neque per ullum numerum primum formae $4n + 3$, diuidi possunt; omnium reliquorum non-residuum. V. artt. 103 et 105.

112. Progredimur ad residua $+2$ et -2.

Si ex tabula II colligimus omnes numeros primos quorum residuum est $+2$, hos habebimus: 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97. Facile autem animaduertitur, inter hos numeros nullos inueniri formarum $8n + 3$ et $8n + 5$.

Videamus itaque, num haec inductio ad certitudinem euehi possit.

Primum obseruamus quemuis numerum compositum formae $8n + 3$ vel $8n + 5$ neces-

*) Quando igitur de numero quocunque loquemur quatenus numeri formae $4n + 1$ residuum vel non-residuum est, ipsius signum omnino negligere siue etiam signum anceps $\pm$ ipsi tribuere poterimus.

sario factorem primum alterutrius formae $8n + 3$ vel $8n + 5$, inuoluere; manifesto enim e solis numeris primis formarum $8n + 1$, $8n + 7$, alii numeri quam qui sunt formae $8n + 1$ vel $8n + 7$, componi nequeunt. Quodsi itaque inducto nostra generaliter est vera, nullus omnino numerus formae $8n + 3$, $8n + 5$ dabitur, cuius residuum $+ 2$; sicque nullus certe numerus huius formae infra 100 exstat, cuius residuum sit -2. Si autem vltra hunc limitem tales numeri repirirentur, ponamus minimum omnium $= t$. Erit itaque t vel formae $8n + 3$ vel $8n + 5$; $+ 2$ ipsius residuum erit, omnium autem numerorum similium minorum non-residuum. Ponatur $2 \equiv aa \pmod{t}$ poteritque a ita semper accipi vt sit impar simulque $< t$, (habebit enim a ad minimum duos valores positiuos ipso t minores quorum summa $= t$, quorumque adeo alter par alter impar v. art. 104. 105). Quo facto sit $aa = 2 + tu$, siue $tu = aa - 2$, eritque aa formae $8n + 1$, tu igitur formae $8n - 1$, adeoque u formae $8n + 3$ vel $8n + 5$, prout t est formae posterioris vel prioris. At ex aequatione $aa = 2 + tu$ sequitur, etiam $2 \equiv a \pmod{u}$ *i. e.* 2 etiam ipsius u residuum fore. Facile vero perspicitur, esse $u < t$; quare t non est minimus numerus inductioni nostrae contrarius contra hyp. Vnde manifesto sequitur id quod per inductionem inueneramus generaliter verum esse.

Combinando haec cum prop. art. 111. sequentia theoremata nanciscimur.