

itaque tot formae diuisorum ipsius $xx - A$, quot dantur formae non-diuisorum, scilicet $\frac{1}{2} (a - 1) (b - 1) (c - 1)$ etc.

149. *Casum secundum et tertium* hic simul contemplari possumus. Poterit scilicet A semper hic poni $= (-1) Q$, aut $= (+2) Q$ aut $= (-2) Q$, designante Q numerorum formae $+(4n + 1)$, aut $-(4n - 1)$, quales in art praec. consideramus. Sit generaliter $A = \alpha Q$, ita vt sit α aut $= -1$, aut $= \pm 2$. Tum erit A residuum omnium numerorum, quorum residuum est aut vterque α et Q , aut neuter; non-residuum autem omnium, quorum non residuum alteruter tantum numerorum α , Q . Hinc formae diuisorum ac non-diuisorum ipsius $xx - A$ facile deriuantur. Si $\alpha = -1$ distribuuntur omnes numeri ipso $4A$ minores ad ipsumque primi in duas classes, in priorem ii, qui sunt in aliqua forma diuisorum ipsius $xx - Q$, simulque in forme $4n + 1$, iique, qui sunt in aliqua forma non-diuisorum ipsius $xx - Q$ simulque in forma $4n + 3$; in posteriorem reliqui. Sint priores r, r', r'' etc., posteriores n, n', n'' etc., eritque A residuum omnium numerorum primorum in aliqua formarum $4Ak + r, 4Ak + r', 4Ak + r''$ etc. contentorum, non-residuum autem omnium primorum in aliqua formarum $4Ak + n, 4Ak + n'$ etc. contentorum. — Si $\alpha = \pm 2$, distribuuntur omnes numeri ipso $8Q$ minores ad ipsumque primi in duas classes, in primam ii, qui continentur in aliqua forma diuisorum ipsius $xx - Q$ simulque in aliqua formarum $8n + 1, 8n$

+ 7 pro signo superiori, vel formarum $8n + 1$, $8n + 3$ pro inferiori, iique qui contenti sunt in aliqua forma non-divisorum ipsius $xx - Q$ simulque in aliqua harum $8n + 3$, $8n + 5$ pro signo superiori, vel harum $8n + 5$, $8n + 7$ pro inferiori, — in secundam reliqui. Tum designatis numeris classis prioris per r , r' , r'' etc., numerisque classis posterioris per n , n' , n'' etc. $\pm 2Q$ erit residuum omnium numerorum primorum in aliqua formarum $8Qk + r$, $8Qk + r'$, $8Qk + r''$ etc. contentorum, omnium autem primorum in aliqua formarum $8Qk + n$, $8Qk + n'$, $8Qk + n''$ etc. non-residuum. Ceterum facile demonstrari potest, etiam hic totidem formas divisorum ipsius $xx - A$ datum iri ac non-divisorum.

Ex. Hoc modo inuenitur ± 10 esse residuum omnium numerorum primorum in aliqua formarum $40k + 1$, 3, 9, 13, 27, 31, 37, 39, contentorum, non-residuum vero omnium primorum, qui sub aliqua formarum $40k + 7$, 11, 17, 19, 21, 23, 29, 33 continentur.

150. Formae hae plures habent proprietates satis memorabiles, quarum tamen vnam tantummodo apponimus. Si B est numerus compositus ad A primus, inter cuius factores primos occurrunt $2m$, qui in aliqua forma non-divisorum ipsius $xx - A$ continentur, B in aliqua forma divisorum ipsius $xx - A$ contentus erit; si vero multitudo factorum primorum ipsius B in aliqua forma non-divisorum ipsius

$xx - A$ contentus erit. Demonstrationem quae non est difficilis omittimus. Hinc vero sequitur, non modo quemuis numerum primum sed etiam quemuis compositum imparem ad A primum, qui in aliqua forma non-diuisorum contineatur, non-diuisorem fore; necessario enim aliquis factor primus talis numeri debet esse non-diuisor.

151. Theorema fundamentale, quod sane inter elegantissima in hoc genere est referendum, in eadem forma simplici, in qua supra propositum est, a nemine hucusque fuit prolatum. Quod eo magis est mirandum, quum aliae quaedam propositiones illi superstruendae ex quibus ad illud facile reueniri potuisset, ill. Eulero iam innotuerint. Formas certas dari, in quibus omnes diuisores primi numerorum formae $xx - A$ contineantur, aliasque in quibus omnes non-diuisores primi numerorum eiusdem formae sint comprehensi, ita vt hae illas excludant, nouerat, methodumque illas formas inueniendi eruerat: sed omnes ipsius conatus ad demonstrationem perueniendi semper irriti fuerunt, veritatisque illi per inductionem inuentae maiorem tantummodo verisimilitudinem conciliauerunt. In aliqua quidem tractatione, *Nouae demonstrationes circa diuisores numerorum formae $xx + nyy$* , quae in Acad. Petrop. recitata est 1775 Nou. 20, et post mortem viri summi in *T. I. Nou. Act.* huius Ac. p. 47 sqq. est conseruata, voti se compotem credidisse videtur: sed hic error irrepsit, scilicet p. 65. *tacite* supposuit, formas tales diuisorum